SIEMENS

SIMATIC NET

Industrial Ethernet Security
Security-Grundlagen und -Anwendung

Projektierungshandbuch

12/2014

C79000-G8900-C286-04

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠GEFAHR
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠WARNUNG
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠VORSICHT
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

⚠WARNUNG
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Dokumentbestellnummer: C79000-G8900-C286-04
Ⓟ 12/2014 Änderungen vorbehalten

Vorwort

Vorwort

Dieses Handbuch…

…unterstützt Sie bei der Projektierung der Security-Funktionalitäten folgender "Security Integrated"-Produkte:

- SCALANCE S: S602 / S612 / S623 / S627-2M
- SOFTNET Security Client
- S7-CPs: CP 343-1 Advanced, CP 443-1 Advanced
- PC-CP: CP 1628
- Mobilfunk-Router: SCALANCE M875
- SCALANCE M-800:
  - ADSL-Router: SCALANCE M81x
  - SHDSL-Router: SCALANCE M82x
  - Mobilfunk-Router: SCALANCE M874-2 sowie SCALANCE M874-3

Allgemeine Benennung "Security-Baugruppe"

In der vorliegenden Dokumentation werden die folgenden Produkte unter der Benennung "Security-Baugruppe" zusammengefasst: SCALANCE S602 / SCALANCE S612 / SCALANCE S623 / SCALANCE S627-2M, CP 343-1 Advanced, CP 443-1 Advanced, CP 1628.

Funktionsunterschiede werden durch Symbole gekennzeichnet (siehe Abschnitt "Symbolerklärungen"). Hardwarebeschreibungen und Hinweise zur Installation finden Sie in den Dokumenten der einzelnen Baugruppen.

Verwendung der Benennungen "Schnittstelle" und "Port"

In der vorliegenden Dokumentation werden die folgenden Benennungen für die Ports von SCALANCE S Baugruppen verwendet:

- "Externe Schnittstelle": Der externe Port beim SCALANCE S602 / S612 / S623 bzw. ein externer Port beim SCALANCE S627-2M (rote Markierung)
- "Interne Schnittstelle": Der interne Port beim SCALANCE S602 / S612 / S623 bzw. ein interner Port beim SCALANCE S627-2M (grüne Markierung)
- "DMZ-Schnittstelle": Der DMZ-Port beim SCALANCE S623 / S627-2M (gelbe Markierung)

Die Benennung "Port" selbst wird dann verwendet, wenn ein spezieller Port einer Schnittstelle im Vordergrund steht.

Allgemeine Benennung "STEP 7"

Die Projektierung der Security-Funktionen von CPs ist ab STEP 7 V5.5 SP2 HF1 möglich. Deshalb wird in der vorliegenden Dokumentation die Benennung "STEP 7" stellvertretend für alle Versionsstände von STEP 7 ab V5.5 SP2 HF1 bis kleiner als STEP 7 V10 verwendet. Wie Sie die Projektierung der Security-Funktionen von allen Security-Baugruppen in STEP 7 ab V12 vornehmen, entnehmen sie in STEP 7 ab V12 dem Informationssystem, Abschnitt "Industrial Ethernet Security".

Allgemeine Benennung "CP x43-1 Adv."

In der vorliegenden Dokumentation werden die folgenden Produkte unter der Benennung "CP x43-1 Adv." zusammengefasst: CP 343-1 Advanced / CP 443-1 Advanced.

Security Configuration Tool V4.1 - Neue Funktionen

Mit dem Security Configuration Tool V4.1 sind die folgenden neuen Funktionen berücksichtigt:

- **Erweiterung der VPN-Funktionalität für SCALANCE M Baugruppen**

  Der aktive VPN-Verbindungsaufbau von einer SCALANCE M Baugruppe zu einer SCALANCE M-800 Baugruppe wird unterstützt.

- **Erweiterung der Funktionalität "Router- und Firewallredundanz" für SCALANCE S623/S627-2M Baugruppen ab Firmware V4.0.1**

  Die Projektierung von virtuellen Router-IDs für die virtuellen Schnittstellen von Redundanzbeziehungen wird für SCALANCE S623/S627-2M Baugruppen ab Firmware V4.0.1 unterstützt.

- **Erweiterung der Firewall-Funktionalität für SCALANCE S Baugruppen ab Firmware V3**

  Die Projektierung von IP-Regeln ohne Firewall-States wird für SCALANCE S Baugruppen ab Firmware V3 unterstützt.

Gültigkeitsbereich dieses Handbuchs

Dieses Handbuch ist für folgende SIMATIC NET Baugruppen gültig:

Baugruppe	MLFB
SCALANCE S602	6GK5 602-0BA10-2AA3
SCALANCE S612	6GK5 612-0BA10-2AA3
SCALANCE S623	6GK5 623-0BA10-2AA3
SCALANCE S627-2M	6GK5 627-2BA10-2AA3
CP 343-1 Advanced ab V3	6GK7 343-1GX31-0XE0
CP 443-1 Advanced ab V3	6GK7 443-1GX30-0XE0
CP 1628	6GK1162-8AA00

Dieses Handbuch ist für folgende SIMATIC NET Projektierungswerkzeuge gültig:

Projektierungswerkzeug	MLFB	Ausgabestand
SOFTNET Security Client	6GK1 704-1VW04-0AA0	V4.0 Hotfix 1
Security Configuration Tool (SCT)	-	V4.1

Leserkreis

Dieses Handbuch wendet sich an Personen, welche die Industrial Ethernet Security-Funktionalitäten in einem Netzwerk einrichten.

SIMATIC NET Manual Collection (Bestell-Nr. A5E00069051)

SCALANCE S Baugruppen, den S7-CPs sowie dem PC-CP 1628 liegt die SIMATIC NET Manual Collection bei. Diese Manual Collection wird in regelmäßigen Abständen aktualisiert; sie enthält die zum Erstellungszeitpunkt aktuellen Gerätehandbücher und Beschreibungen.

Marken

Folgende und eventuell weitere nicht mit dem Schutzrechtsvermerk ® gekennzeichnete Bezeichnungen sind eingetragene Marken der Siemens AG:

C-PLUG, CP 343-1, CP 443-1, Industrial Ethernet, SCALANCE, SIMATIC NET, SOFTNET

In dieser Anleitung verwendete Symbole

S≥V3.0

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE S ab V3.0 relevant.

S≥V4.0

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE S ab V4.0 relevant.

SCA. S

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE S relevant.

SCA. M

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE M relevant.

M875

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle Baugruppen außer SCALANCE M875 relevant.

SCA-M

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle Baugruppen außer SCALANCE M relevant.



Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle Security-Baugruppen außer SCALANCE S602 relevant.

S<V3.0

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle Security-Baugruppen außer SCALANCE S < V3.0 relevant.

S602 ≥V3.1

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE S602 ab V3.1 relevant.

S623

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE S623 relevant.

S627-2M

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE S627-2M relevant.

S62x

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE S623 und SCALANCE S627-2M relevant.

S62x ≥ V4.0

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE S623 ab V4.0 und SCALANCE S627-2M ab V4.0 relevant.

S7-CP

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für S7-CPs relevant.

S7-CP

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle Security-Baugruppen außer den S7-CPs relevant.

PC-CP

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für PC-CPs relevant.



Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle Security-Baugruppen außer den PC-CPs relevant.



Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle S7-CPs und PC-CPs relevant.



Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle Security-Baugruppen außer den CPs relevant.



Das Symbol verweist auf besondere Literaturempfehlungen.



Dieses Symbol weist auf detailliertere Hilfestellung in der kontextabhängigen Hilfe hin. Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

Literaturhinweise /.../

Hinweise auf weitere Dokumentationen sind mit Hilfe von Literaturnummern in Schrägstrichen /.../ angegeben. Anhand dieser Nummern können Sie dem Literaturverzeichnis am Ende des Handbuchs den Titel der Dokumentation entnehmen.

Siehe auch

Customer-Support-Seiten (http://support.automation.siemens.com/WW/view/de/18701555/130000)

SIMATIC NET-Glossar

Erklärungen zu vielen Fachbegriffen, die in dieser Dokumentation vorkommen, sind im SIMATIC NET-Glossar enthalten.

Sie finden das SIMATIC NET-Glossar hier:

- SIMATIC NET Manual Collection oder Produkt-DVD

  Die DVD liegt einigen SIMATIC NET-Produkten bei.

- Im Internet unter folgender Beitrags-ID:

  50305045 (http://support.automation.siemens.com/WW/view/de/50305045)

Inhaltsverzeichnis

1 Einführung und Grundlagen

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Lösungen, Maschinen, Geräten und/oder Netzwerken unterstützen. Sie sind wichtige Komponenten in einem ganzheitlichen Industrial Security-Konzept. Die Produkte und Lösungen von Siemens werden unter diesem Gesichtspunkt ständig weiterentwickelt. Siemens empfiehlt, sich unbedingt regelmäßig über Produkt-Updates zu informieren.

Für den sicheren Betrieb von Produkten und Lösungen von Siemens ist es erforderlich, geeignete Schutzmaßnahmen (z. B. Zellenschutzkonzept) zu ergreifen und jede Komponente in ein ganzheitliches Industrial Security-Konzept zu integrieren, das dem aktuellen Stand der Technik entspricht. Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen. Weitergehende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Um stets über Produkt-Updates informiert zu sein, melden Sie sich für unseren produktspezifischen Newsletter an. Weitere Informationen hierzu finden Sie unter http://support.automation.siemens.com.

1.1 Wichtige Hinweise

Allgemein

Hinweis

Schutz vor unberechtigtem Zugriff

Achten Sie darauf, dass der Projektierungsrechner (PC/PG) bzw. das Projekt vor unberechtigtem Zugriff geschützt ist.

Hinweis

Gastkonto deaktivieren

Stellen Sie sicher, dass das Gastkonto auf dem Projektierungsrechner deaktiviert ist.

Hinweis

Aktuelles Datum und aktuelle Uhrzeit auf den Security-Baugruppen

Achten Sie bei der Verwendung von gesicherter Kommunikation (z. B. HTTPS, VPN...) darauf, dass die betroffenen Security-Baugruppen über die aktuelle Uhrzeit und das aktuelle Datum verfügen. Die verwendeten Zertifikate werden sonst als nicht gültig ausgewertet und die gesicherte Kommunikation funktioniert nicht.

Hinweis

Aktuelle Antiviren-Software

Es wird empfohlen, dass auf allen Projektierungsrechnern immer eine aktuelle Antiviren-Software installiert und aktiviert ist.

Hinweis

FTPS

Wird in der vorliegenden Dokumentation die Benennung "FTPS" verwendet, ist damit FTPS im expliziten Modus gemeint (FTPES).

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sie können eine einmal vorgenommene Umschaltung in den Erweiterten Modus für das aktuelle Projekt nicht mehr rückgängig machen.

Abhilfe für SCT Standalone: Schließen Sie das Projekt ohne zu speichern und öffnen Sie es erneut.

Hinweis

Zusätzliche Security-Maßnahmen bei der Verwendung des SOFTNET Security Clients

Der SOFTNET Security Client bietet eine Lösung für die sichere Kommunikation mit Automatisierungszellen über VPN. Für den Eigenschutz des PCs/PGs sowie der damit verbundenen Automatisierungszelle wird empfohlen, zusätzliche Maßnahmen wie z.B. Virenscanner sowie die Windows-Firewall einzusetzen.

Unter Windows 7 muss die Firewall des Betriebssystems aktiviert sein, damit der VPN-Tunnelaufbau funktioniert.

CP x43-1 Adv.

Hinweis

Zusätzliche Sicherheitseinstellungen

Um zu vermeiden, dass unautorisierte Projektierungsdaten in den CP geladen werden, müssen Sie zusätzliche Sicherheitseinstellungen an der Firewall des CPs vornehmen (z.B. Blocken der S7-Kommunikation oder Zulassen von ausschließlich getunnelter Kommunikation) bzw. externe Sicherheitsmaßnahmen ergreifen.

STEP 7

Hinweis

"Speichern und Übersetzen" nach Änderungen

Damit die Security-Einstellungen in die entsprechenden (Offline-)Systemdatenbausteine übernommen werden, wählen Sie nach vorgenommenen Änderungen das Menü "Station" > "Speichern und Übersetzen" in HW Konfig bzw. "Netz" > "Speichern und Übersetzen" in NetPro.

Hinweis

Öffnen einer Station bei geöffnetem Security Configuration Tool

Schließen Sie das Security Configuration Tool, bevor Sie eine weitere Station über den SIMATIC Manager oder NetPro öffnen.

Hinweis

Keine STEP 7 Multiprojekte in Verbindung mit Security

Für jedes STEP 7 Projekt wird beim Aktivieren von Security eine eigene eindeutige Security-Konfiguration erstellt. STEP 7 Multiprojekte werden daher in Verbindung mit Security nicht unterstützt.

1.2 Einführung und Grundlagen

Mit den SIMATIC NET Security-Baugruppen und dem SIMATIC NET SOFTNET Security Client haben Sie sich für das SIEMENS Sicherheitskonzept entschieden, das den hohen Anforderungen geschützter Kommunikation in der industriellen Automatisierungstechnik gerecht wird.

Hinweis

Aktuelle Antiviren-Software

Es wird empfohlen, dass auf allen Projektierungsrechnern immer eine aktuelle Antiviren-Software installiert ist.

Dieses Kapitel gibt Ihnen einen Überblick über die Sicherheitsfunktionen der Geräte und Komponenten:

- SCALANCE S
- CP x43-1 Adv.
- CP 1628
- SOFTNET Security Client

Tipp:

Den schnellen Einstieg mit den Security-Baugruppen finden Sie im Dokument "SIMATIC NET Security - Getting Started".

1.3 Produkteigenschaften

1.3.1 Funktionsübersicht

Funktionsübersicht der Baugruppentypen

Entnehmen Sie der folgenden Tabelle, welche Funktionen die einzelnen Security-Baugruppen unterstützen.

Hinweis

In diesem Handbuch werden alle Funktionen beschrieben. Berücksichtigen Sie anhand der nachfolgenden Tabelle, welche Funktionen auf die von Ihnen genutzte Security-Baugruppe zutreffen.

Achten Sie auch auf die zusätzlichen Angaben in den Kapitelüberschriften.

Tabelle 1- 1 Funktionsübersicht

Funktion	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V4.0
Projektierung über			
Security Configuration Tool	-	-	x
Security Configuration Tool in STEP 7 integriert	x	x	x
Kompatibilität zu IP Access Control-Listen (ACL)	x	-	-
Allgemein			
NAT-/NAPT-Router	x	-	x
NAT-/NAPT-Routing in VPN-Verbindungen	-	-	x S602
DHCP-Server	-	-	x
Firewall			
Lokale Firewall-Regeln	x	x	x
Globale Firewall-Regelsätze	x	x	x
Benutzerspezifische IP-Regelsätze	-	-	x
IPsec			
Aufbau von IPsec-Tunneln	x	x	x S602
Benutzerverwaltung			
Benutzerverwaltung	x	x	x
Migration der aktuellen Benutzerver-waltung	x	-	x
Benutzerauthentifizierung durch RADIUS-Server	-	-	x
Unterstützte Protokolle			
SNMPv3	x	x	x
HTTPS-Server	x	-	x
FTPS-Server	x	-	-
FTPS-Client	x	-	-
NTP-Client	x	x	x
NTP-Client (gesichert)	x	x	x
PPPoE-Client	-	-	x
DDNS-Client / DNS-Client	-	-	x
LLDP	x	-	x
MRP-/HRP-Client	-	-	x S627-2M
Logging			
Aufzeichnung von System-Ereignissen	x	x	x
Aufzeichnung von Audit-Ereignissen	x	x	x

Funktion	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V4.0
Aufzeichnung von Paketfilter-Ereignissen	x	x	x
Audit-Meldungen in den Diagnosepuffern der Security-Baugruppe	x	x	-
Zugriff über Security Configuration Tool auf Log-Puffer der Security-Baugruppe	x	x	x
Diagnose über Security Configuration Tool	x	x	x
Senden der Meldungen an Syslog-Server	x	x	x
Web-Diagnose	x	-	-
Ghost-Modus			
Ermittlung der IP-Adresse des internen Teilnehmers zur Laufzeit und Übernahme der IP-Adresse für den externen Port der Security-Baugruppe	-	-	x S602 ≥V3.1
Demilitarisierte Zone (DMZ)			
Einrichtung einer DMZ zur Entkopplung des sicheren Netzes vom unsicheren Netz	-	-	x S62x
Router- und Firewallredundanz			
Redundante Ausführung von Security-Baugruppen zur Erhaltung der Router- und Firewallfunktionalität bei Ausfall einer Security-Baugruppe	-	-	x S62x ≥ V4.0

x Funktion wird unterstützt

- Funktion wird nicht unterstützt

1.3.2 Mengengerüste

Hinweis

Eine komplette Übersicht der zulässigen Mengengerüste finden Sie im Internet unter folgender Adresse: (http://support.automation.siemens.com/WW/view/de/58217657).

Mengengerüste

Funktion	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V4.0
VPN-Tunnel pro Security-Baugruppe	Max. 32	Max. 64	Max. 128
Firewall-Regeln pro Security-Baugruppe	Max. 256		
Projektweit anlegbare NTP-Server (zuweisbare NTP-Server pro Security-Baugruppe)	32 (4)		

1.3.3 Regeln für Benutzernamen, Rollen und Passwörter

Welche Regeln gelten für Benutzernamen, Rollennamen und Passwörter?

Beachten Sie beim Anlegen oder Ändern eines Benutzers, einer Rolle oder eines Passworts die folgenden Regeln:

<table>
<tr><td>Erlaubte Zeichen</td><td>Erlaubt sind folgende Zeichen des Zeichensatzes ANSI X 3.4-1986:
0123456789
A...Z a...z
!#$%&()*+,-./:;<=>?@ [\]_{|}~^</td></tr>
<tr><td>Nicht erlaubte Zeichen</td><td>" ' ` §</td></tr>
<tr><td>Länge des Benutzernamens (Authentifizierungsmethode "Passwort")</td><td>1 ... 32 Zeichen</td></tr>
<tr><td>Länge des Benutzernamens (Authentifizierungsmethode "RADIUS")</td><td>1 ... 255 Zeichen</td></tr>
<tr><td>Länge des Passworts</td><td>8 ... 32 Zeichen</td></tr>
<tr><td>Länge des Rollennamens</td><td>1 ... 32 Zeichen</td></tr>
<tr><td>Maximale Benutzeranzahl pro Projekt</td><td>128</td></tr>
<tr><td>Maximale Benutzeranzahl auf einer Security-Baugruppe</td><td>32 + 1 Administrator beim Anlegen des Projekts</td></tr>
<tr><td>Maximale Rollenanzahl pro Projekt</td><td>128 (122 benutzerdefinierte + 6 systemdefinierte)</td></tr>
<tr><td>Maximale Rollenanzahl auf einer Security-Baugruppe</td><td>37 (31 benutzerdefinierte + 6 systemdefinierte)</td></tr>
</table>

Hinweis

Benutzernamen und Passwörter

Als wichtige Maßnahme zur Erhöhung der Sicherheit achten Sie stets darauf, dass Benutzernamen und Passwörter möglichst lang sind und Sonderzeichen, Groß-/Kleinschreibung sowie Zahlen enthalten.

Mit Hilfe von Passwort-Richtlinien können Sie die oben aufgeführten Restriktionen für Passwörter weiter einschränken. Wie Sie Passwort-Richtlinien definieren, erfahren Sie im Kapitel:
Passwort-Richtlinien projektieren (Seite 76)

Passwortstärke

Bei der Eingabe eines neuen Passworts wird dessen Passwortstärke überprüft. Folgende Stufen werden bei der Passwortstärke unterschieden:

- Sehr schwach
- Schwach
- Mittel
- Gut
- Stark
- Sehr stark

Hinweis

Passwortstärke von bereits bestehenden Benutzern überprüfen

Überprüfen Sie die Passwortstärke

- von bereits im Projekt vorhandenen Benutzern,
- des ersten in STEP 7 angelegten Benutzers,
- von migrierten Benutzern,

indem Sie in der Benutzerverwaltung im Register "Benutzer" den jeweiligen Benutzer selektieren und auf die Schaltfläche "Bearbeiten..." klicken.

1.3.4 Baugruppe austauschen



So erreichen Sie diese Funktion

1. Markieren Sie die zu bearbeitende Security-Baugruppe bzw. den zu bearbeitenden SOFTNET Security Client.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Baugruppe austauschen…".
3. Abhängig vom Produkttyp und dem Firmwarerelease der gewählten Baugruppe können Sie in dem Dialog den Baugruppentyp und/oder das Firmwarerelease anpassen.

Entnehmen Sie der nachfolgenden Tabelle, welche Baugruppen Sie ohne und mit eventuellen Datenverlusten austauschen können.

Hinweis

Ersetzen von CPs

Informationen zum Ersetzen von CPs finden Sie im jeweiligen Gerätehandbuch.

Ausgangs-baugruppe	Möglicher Baugruppentausch											
	S602 V2	S602 V3	S602 V4	S612 V1	S612 V2	S612 V3	S612 V4	S613 V1	S613 V2	S623 V3	S623 V4	S627-2M V4
S602 V2	-	x	x	!	x	x	x	!	x	x	x	x
S602 V3	!	-	x	!	!	!	!	!	!	!	!	!
S602 V4	!	!	-	!	!	!	!	!	!	!	!	!
S612 V1	!	!	!	-	x	x	x	x	x	x	x	x
S612 V2	!	!	!	!	-	x	x	!	x	x	x	x
S612 V3	!	!	!	!	!	-	x	!	!	x	x	x
S612 V4	!	!	!	!	!	!	-	!	!	x	x	x
S613 V1	!	!	!	!	!	x	x	-	x	x	x	x
S613 V2	!	!	!	!	!	x	x	!	-	x	x	x
S623 V3	!	!	!	!	!	!	!	!	!	-	x	x
S623 V4	!	!	!	!	!	!	!	!	!	!	-	x
S627-2M V4	!	!	!	!	!	!	!	!	!	!	!	-

x Ohne Verluste

! Mit eventuellen Verlusten

- Der Baugruppentyp und die Firmwareversion werden nicht geändert.

Ausgangskonfiguration	Möglicher Tausch			
	SOFTNET Security Client 2005	SOFTNET Security Client 2008	SOFTNET Security Client V3.0	SOFTNET Security Client V4.0
SOFTNET Security Client 2005	-	x	x	x
SOFTNET Security Client 2008	x*	-	x	x
SOFTNET Security Client V3.0	x* **	x**	-	x
SOFTNET Security Client V4.0	x* **	x**	x	-

***** Wenn sich der SOFTNET Security Client nicht in einer Routing-Gruppe befindet.

****** Wenn sich der SOFTNET Security Client nicht mit einer SCALANCE M Baugruppe in einer VPN-Gruppe befindet.

Siehe auch

Bedienoberfläche und Menübefehle (Seite 47)

/2/ (Seite 278)

1.4 Einsatz des SOFTNET Security Clients

PG/PC-Kommunikation im VPN - Aufgabe des SOFTNET Security Client

Mit der PC-Software SOFTNET Security Client sind gesicherte Fernzugriffe vom PG/PC auf Automatisierungsgeräte, die durch Security-Baugruppen geschützt sind, über öffentliche Netze hinweg möglich.

Mittels des SOFTNET Security Client wird ein PG/PC automatisch so konfiguriert, dass er eine gesicherte IPsec-Tunnelkommunikation im VPN (Virtual Private Network) zu einer oder mehreren Security-Baugruppen aufbauen kann.

PG/PC-Applikationen wie NCM Diagnose oder STEP 7 können so über eine gesicherte Tunnelverbindung auf Geräte oder Netzwerke zugreifen, die sich in einem durch Security-Baugruppen geschützten internen Netz befinden.

Die PC-Software SOFTNET Security Client wird ebenfalls mit dem Projektierwerkzeug Security Configuration Tool konfiguriert; damit ist eine durchgängige Projektierung gewährleistet.

1.5 Einsatz von SCALANCE S602

Firewall und Router - Aufgabe von SCALANCE S602

Durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall und NAT/NAPT-Router schützt die Security-Baugruppe SCALANCE S602 einzelne Geräte oder auch ganze Automatisierungszellen vor:

- Datenspionage
- unerwünschten Zugriffen

SCALANCE S602 ermöglicht diesen Schutz flexibel und ohne komplizierte Handhabung.

SCALANCE S602 wird mit dem Projektierwerkzeug Security Configuration Tool konfiguriert.

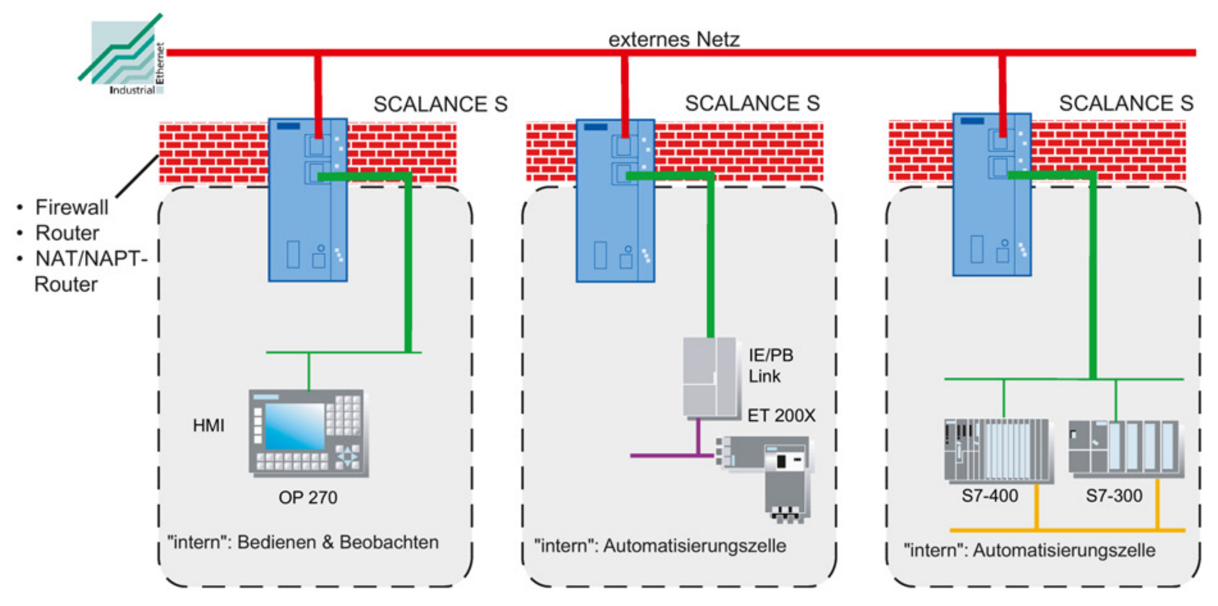


Bild 1-1 Netzkonfiguration mit SCALANCE S602

Sicherheitsfunktionen

- Firewall
  - IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
  - Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3

    (Layer-2-Telegramme; gilt nicht für S602, wenn der Router-Betrieb genutzt wird);
  - Bandbreitenbegrenzung
  - Globale Firewall-Regelsätze
  - Benutzerspezifische IP-Regelsätze

  Alle Netzknoten, die sich im internen Netzsegment eines SCALANCE S befinden, werden durch dessen Firewall geschützt.
- Router-Betrieb

  Indem Sie SCALANCE S als Router betreiben, entkoppeln Sie das interne Netz vom externen Netz. Das von SCALANCE S verbundene interne Netz wird somit zu einem eigenen Subnetz; SCALANCE S muss als Router explizit über seine IP-Adresse adressiert werden.
- Schutz für Geräte und Netzsegmente

  Die Schutzfunktion Firewall kann sich über den Betrieb einzelner Geräte, mehrerer Geräte wie auch ganzer Netzsegmente erstrecken.
- Rückwirkungsfreiheit beim Einbau in flache Netze (Bridge-Betrieb)

  Beim Einbau eines SCALANCE S602 in eine bestehende Netzinfrastruktur müssen die Endgeräte nicht neu eingestellt werden.
- Security-Baugruppe und interner Teilnehmer als eine Einheit (Ghost-Betrieb)

  Die Security-Baugruppe tritt nach außen mit der IP-Adresse des internen Teilnehmers und der MAC-Adresse der Security-Baugruppe auf.
- NTP (gesichert) S≥V4.0

  Zur sicheren Uhrzeitsynchronisation und -übertragung.

Interne und Externe Netzknoten

SCALANCE S602 teilt Netzwerke in zwei Bereiche auf:

- internes Netz: geschützte Bereiche mit den "internen Knoten"

  Interne Knoten sind alle diejenigen Knoten, die von einem SCALANCE S abgesichert sind.

- externes Netz: ungeschützte Bereiche mit den "externen Knoten"

  Externe Knoten sind alle Knoten, die sich außerhalb der geschützten Bereiche befinden.

Hinweis

Die internen Netze werden als sicher (vertrauenswürdig) betrachtet.

Verbinden Sie ein internes Netzsegment nur über SCALANCE S mit den externen Netzsegmenten.

Weitere Verbindungswege zwischen dem internen und externen Netz dürfen nicht vorhanden sein!

1.6 Einsatz von SCALANCE S612, S623 und S627-2M

Umfassender Schutz - Aufgabe von SCALANCE S612, SCALANCE S623 und SCALANCE S627-2M

Durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall, NAT-/NAPT-Router und VPN (Virtual Private Network) über IPsec-Tunnel schützen die Security-Baugruppen SCALANCE S612, SCALANCE S623 und SCALANCE S627-2M einzelne Geräte oder auch ganze Automatisierungszellen vor:

- Datenspionage
- Datenmanipulation
- unerwünschten Zugriffen

SCALANCE S ermöglicht diesen Schutz flexibel, rückwirkungsfrei, protokollunabhängig (ab Layer-2 gemäß IEEE 802.3) und ohne komplizierte Handhabung.

SCALANCE S und SOFTNET Security Client werden mit dem Projektierwerkzeug Security Configuration Tool konfiguriert.

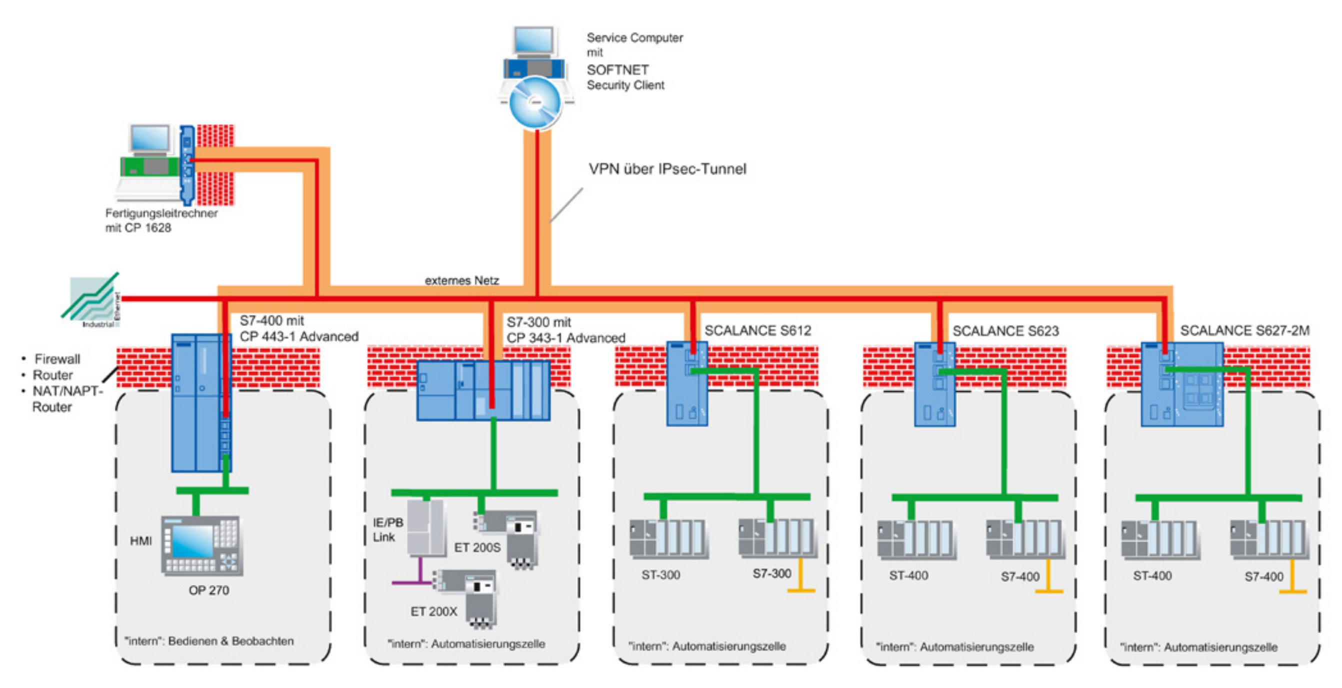


Bild 1-2 Netzkonfiguration mit SCALANCE S612, SCALANCE S623 und SCALANCE S627-2M

Sicherheitsfunktionen

- Firewall
  - IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
  - Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3

    (Layer-2-Telegramme; steht nicht zur Verfügung, wenn der Router-Betrieb genutzt wird)
  - Bandbreitenbegrenzung
  - Globale Firewall-Regelsätze
  - Benutzerspezifische IP-Regelsätze

  Alle Netzknoten, die sich im internen Netzsegment eines SCALANCE S befinden, werden durch dessen Firewall geschützt.
- Gesicherte Kommunikation durch IPsec-Tunnel

  SCALANCE S kann mit anderen Security-Baugruppen per Projektierung zu Gruppen zusammengefasst werden. Zwischen allen Security-Baugruppen einer VPN-Gruppe werden IPsec-Tunnel aufgebaut (VPN, Virtual Private Network). Alle internen Knoten dieser Security-Baugruppen können mittels dieser Tunnel gesichert miteinander kommunizieren.
- Protokollunabhängigkeit

  Die Tunnelung umfasst auch Ethernet-Telegramme gemäß IEEE 802.3 (Layer-2-Telegramme; gilt nicht, wenn der Router-Betrieb genutzt wird).

  Durch die IPsec-Tunnel werden sowohl IP-, als auch Non-IP-Telegramme übertragen.
- PPPoE

  Point to Point Protocol over Ethernet (RFC 2516) zum automatischen Bezug von IP-Adressen vom Provider, so dass der Einsatz eines separaten DSL-Routers entfallen kann.
- Client für dynamisches DNS (DDNS-Client)

  Dynamischer Domain Name Service zur Verwendung dynamischer IP-Adressen, wenn ein SCALANCE S bei Fernwartungsszenarien in Verbindung mit dem SOFTNET Security Client, SCALANCE M Baugruppen, SCALANCE S Baugruppen oder anderen VPN-Clients als VPN-Server eingesetzt wird.
- SNMPv3

  Zur abhörsicheren Übertragung von Netzwerkanalyseinformationen.
- Router-Betrieb

  Indem Sie SCALANCE S als Router betreiben, verbinden Sie das interne Netz mit dem externen Netz. Das über SCALANCE S verbundene interne Netz wird somit zu einem eigenen Subnetz.
- Schutz für Geräte und Netzsegmente

  Die Schutzfunktion Firewall und VPN kann sich über den Betrieb einzelner Geräte, mehrerer Geräte wie auch ganzer Netzsegmente erstrecken.

- Zusätzliche DMZ-Schnittstelle S62x

  In einer demilitarisierten Zone (DMZ) können Server platziert werden, für welche der Zugriff aus anderen Netzen (unsicheres externes Netzwerk, sicheres internes Netzwerk) kontrolliert und eingeschränkt werden kann. So können gesichert beiden Netzwerken entsprechende Dienste und Daten zur Verfügung gestellt werden, ohne den beiden Netzen eine direkte Kommunikation untereinander zu ermöglichen.

- Rückwirkungsfreiheit beim Einbau in flache Netze (Bridge-Betrieb)

  Interne Netzknoten können ohne Projektierung gefunden werden. Beim Einbau eines SCALANCE S in eine bestehende Netzinfrastruktur müssen daher die Endgeräte nicht neu konfiguriert werden.

  Die Security-Baugruppe versucht interne Teilnehmer zu finden; interne Teilnehmer, die auf diesem Weg nicht gefunden werden können, müssen dennoch projektiert werden.

- Benutzerauthentifizierung durch RADIUS-Server S≥V4.0

  Auf einem RADIUS-Server können Benutzernamen, Passwörter und Rollen von Benutzern zentral abgelegt werden. Die Authentifizierung dieser Benutzer erfolgt dann durch den RADIUS-Server.

- NTP (gesichert) S≥V4.0

  Zur sicheren Uhrzeitsynchronisation und -übertragung.

Interne Netzknoten, externe Netzknoten, DMZ-Netzknoten

SCALANCE S teilt Netzwerke in mehrere Bereiche auf:

- Internes Netz: geschützte Bereiche mit den "internen Knoten"

  Interne Knoten sind alle Knoten, die von einem SCALANCE S abgesichert sind.

- Externes Netz: ungeschützte Bereiche mit den "externen Knoten"

  Externe Knoten sind alle Knoten, die sich außerhalb der geschützten Bereiche befinden.

- DMZ-Netz: geschützte Bereiche mit den "DMZ-Knoten" S62x

  DMZ-Knoten sind alle Knoten, die sich in der DMZ befinden und von einem SCALANCE S abgesichert sind.

Hinweis

Die an der internen Schnittstelle angeschlossenen Netze werden als sicher (vertrauenswürdig) betrachtet.

Verbinden Sie ein internes Netzsegment nur über SCALANCE S mit Netzsegmenten eines anderen Sicherheitsniveaus (externes Netz, DMZ-Netz).

Weitere Verbindungswege zwischen dem internen Netz und einem Netz mit anderem Sicherheitsniveau dürfen nicht vorhanden sein.

1.7 Einsatz der DMZ-Schnittstelle von SCALANCE S623 und SCALANCE S627-2M

Einsatzszenarien der DMZ-Schnittstelle

Zusätzlich zu den Funktionen des SCALANCE S612 ist der SCALANCE S623 und der SCALANCE S627-2M mit einer dritten Schnittstelle (DMZ) ausgestattet, an welcher ein zusätzliches Netzwerk angebunden werden kann.
Die Schnittstelle kann in Abhängigkeit vom Einsatzszenario verschiedene Funktionen erfüllen (nicht gleichzeitig):

- Einrichtung einer DMZ
- Endpunkt für VPN-Tunnelverbindung
- Synchronisationsschnittstelle für Router- und Firewallredundanz
- ...

Einrichtung einer DMZ

Mit dem SCALANCE S623 und dem SCALANCE S627-2M lässt sich an der zusätzlichen Schnittstelle eine DMZ (Demilitarisierte Zone) einrichten. Eine DMZ wird häufig dann eingesetzt, wenn Dienste für ein unsicheres Netz bereitgestellt werden sollen und das sichere Netz, das Daten für diese Dienste liefert, von dem unsicheren Netz entkoppelt sein muss.

In der DMZ können beispielsweise Terminal-Server mit installierter Wartungs- und Diagnosesoftware stehen, die zugelassene Anwender aus dem externen Netz nutzen können.

In typischen DMZ-Anwendungsfällen sollte der Anwender die Firewall-Regeln so projektieren, dass vom Internet (extern) Zugriffe auf die Server in der DMZ möglich sind (ggf. noch zusätzlich abgesichert durch einen VPN-Tunnel), nicht aber auf Geräte im gesicherten Bereich (intern).

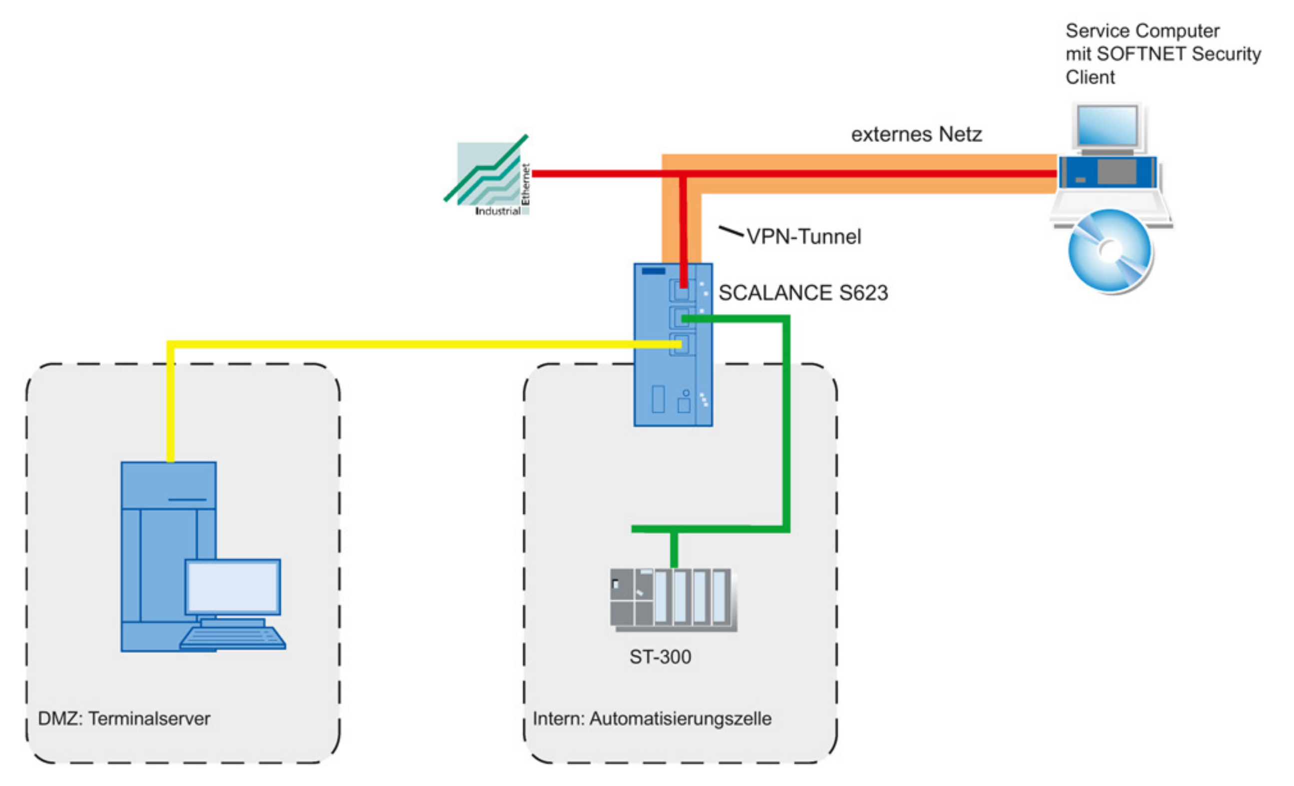


Bild 1-3 Einrichtung einer DMZ

Eine exemplarische Konfiguration, in welcher die DMZ-Schnittstelle zur Einrichtung einer DMZ genutzt wird, wird im Kapitel "4.2 SCALANCE S als Firewall zwischen externem Netz und DMZ" des Handbuchs "SIMATIC NET Industrial Ethernet Security - Security einrichten" durchgeführt.

Endpunkt für VPN-Tunnelverbindung

Die DMZ-Schnittstelle kann als Endpunkt eines VPN-Tunnels genutzt werden. In diesem Szenario ist die DMZ-Schnittstelle über ein angeschlossenes DSL-Modem mit dem Internet verbunden und wird über PPPoE betrieben. Der VPN-Tunnel ermöglicht die sichere Kommunikation mit beispielsweise einer Automatisierungseinheit, die an der internen Schnittstelle einer weiteren Security-Baugruppe angeschlossen ist.

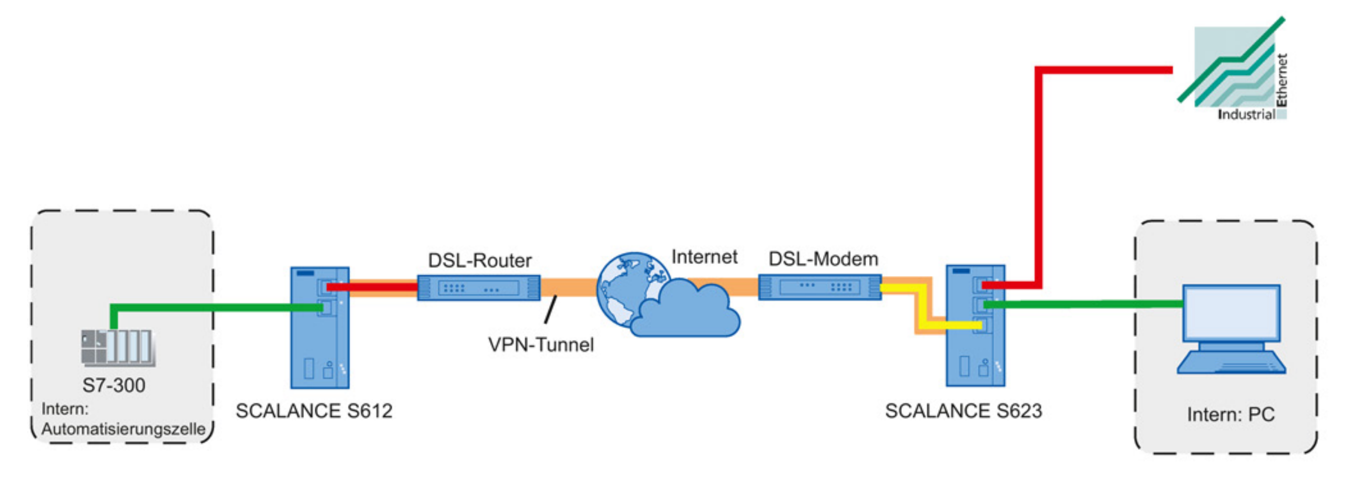


Bild 1-4 Endpunkt für VPN-Tunnelverbindung

Eine exemplarische Konfiguration, in welcher die DMZ-Schnittstelle als Endpunkt eines VPN-Tunnels genutzt wird, wird im Kapitel "5.2 VPN-Tunnel zwischen SCALANCE S623 und SCALANCE S612" des Handbuchs "SIMATIC NET Industrial Ethernet Security - Security einrichten" durchgeführt.

Synchronisationsschnittstelle für Router- und Firewallredundanz S62x ≥ V4.0

Mit dem Einsatz von zwei Security-Baugruppen des Typs SCALANCE S623 oder SCALANCE S627-2M kann der Ausfall einer Security-Baugruppe durch Router- und Firewall-Redundanz kompensiert werden. Hierbei werden beide Security-Baugruppen im Routing-Modus betrieben und jeweils mit dem externen und internen Netz verbunden, wobei stets nur eine Security-Baugruppe aktiv ist. Fällt die aktive Security-Baugruppe aus, übernimmt die passive Security-Baugruppe deren Funktion als Router bzw. Firewall. Um ein funktional identisches Verhalten beider Security-Baugruppen zu gewährleisten, werden die beiden Security-Baugruppen über deren DMZ-Schnittstellen miteinander verbunden und während des Betriebs in ihrer Konfiguration synchronisiert.

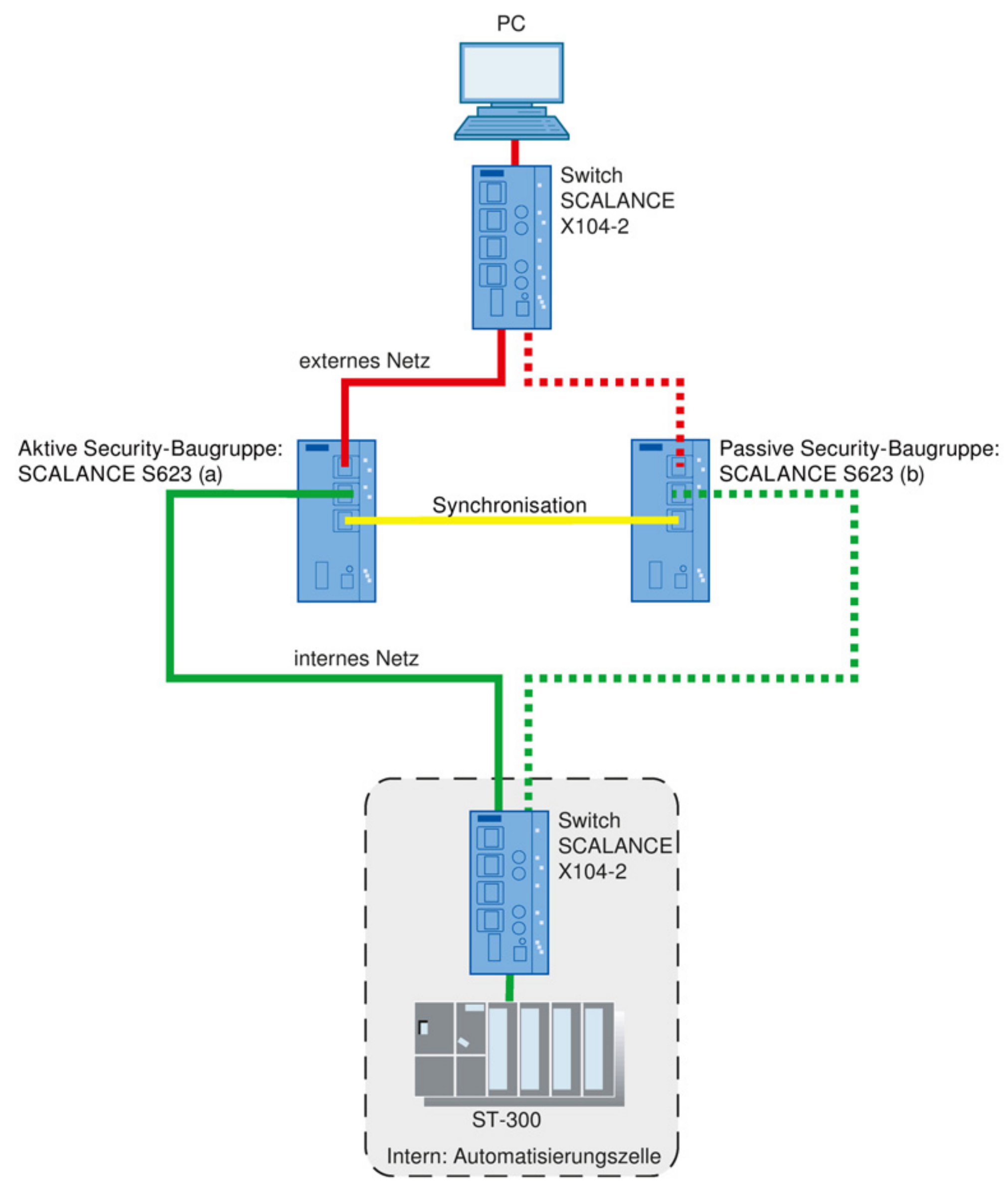


Bild 1-5 Router- und Firewallredundanz

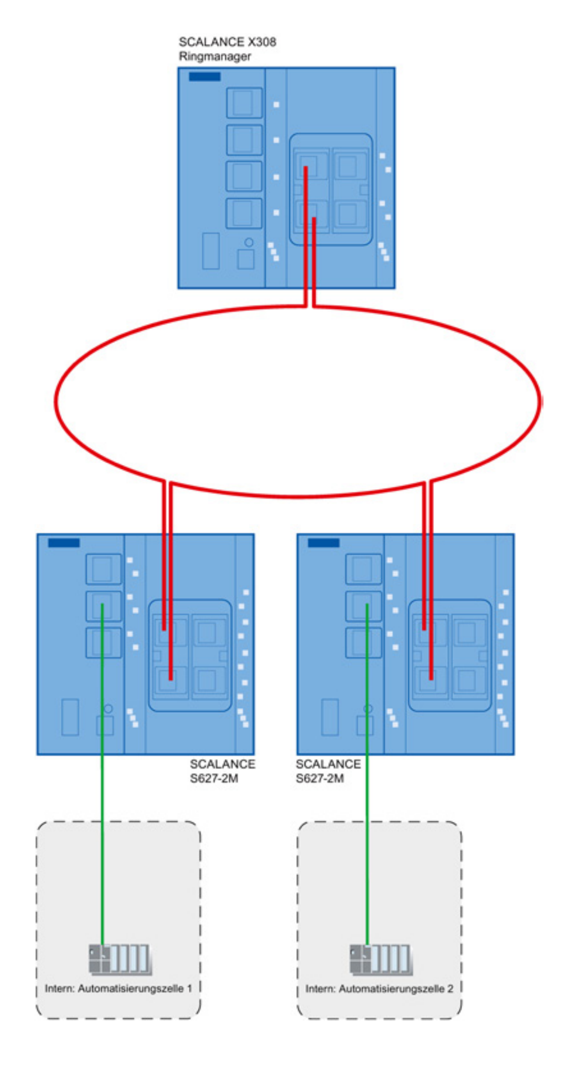
1.8 Einsatz der Medienmodulports von SCALANCE S627-2M

Integration in Ringtopologien

Zusätzlich zu den Funktionen des SCALANCE S623 besitzt der SCALANCE S627-2M zwei Medienmodulslots, in die jeweils ein elektrisches oder optisches Medienmodul mit zwei Ports eingesetzt werden kann. Dadurch wird die externe und die interne Schnittstelle um jeweils bis zu zwei Ports erweitert. Im Routing-Modus können die zusätzlichen Ports der Security-Baugruppe für die Anbindung der externen und internen Schnittstelle an Ringtopologien verwendet werden.

Ringredundanz mit MRP oder HRP

Der SCALANCE S627-2M unterstützt die Protokolle MRP und HRP auf den Medienmodulports der externen und internen Schnittstelle als Client. Als Teilnehmer eines MRP-/HRP-Rings kann ein SCALANCE S627-2M eine unterlagerte Automatisierungszelle oder einen unterlagerten Ring schützen. Diese Sicherung kann auch redundant erfolgen. Leitungsausfälle werden von einem separaten Ringmanager, beispielsweise einem SCALANCE X308, erkannt und durch Umleitung des Kommunikationswegs kompensiert.



1.9 Einsatz von CP 343-1 Advanced und CP 443-1 Advanced

Zellenschutzkonzept - Aufgabe von CP x43-1 Adv.

Mit Industrial Ethernet Security können einzelne Geräte, Automatisierungszellen oder Netzsegmente eines Ethernet-Netzwerks abgesichert werden. Zusätzlich kann die Datenübertragung durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall, NAT-/NAPT-Router und VPN (Virtual Private Network) über IPsec-Tunnel geschützt werden vor:

- Datenspionage
- Datenmanipulation
- unerwünschten Zugriffen

Die Security-Funktionen vom CP x43-1 Adv. werden mit dem Projektierwerkzeug Security Configuration Tool konfiguriert, das in STEP 7 integriert ist.

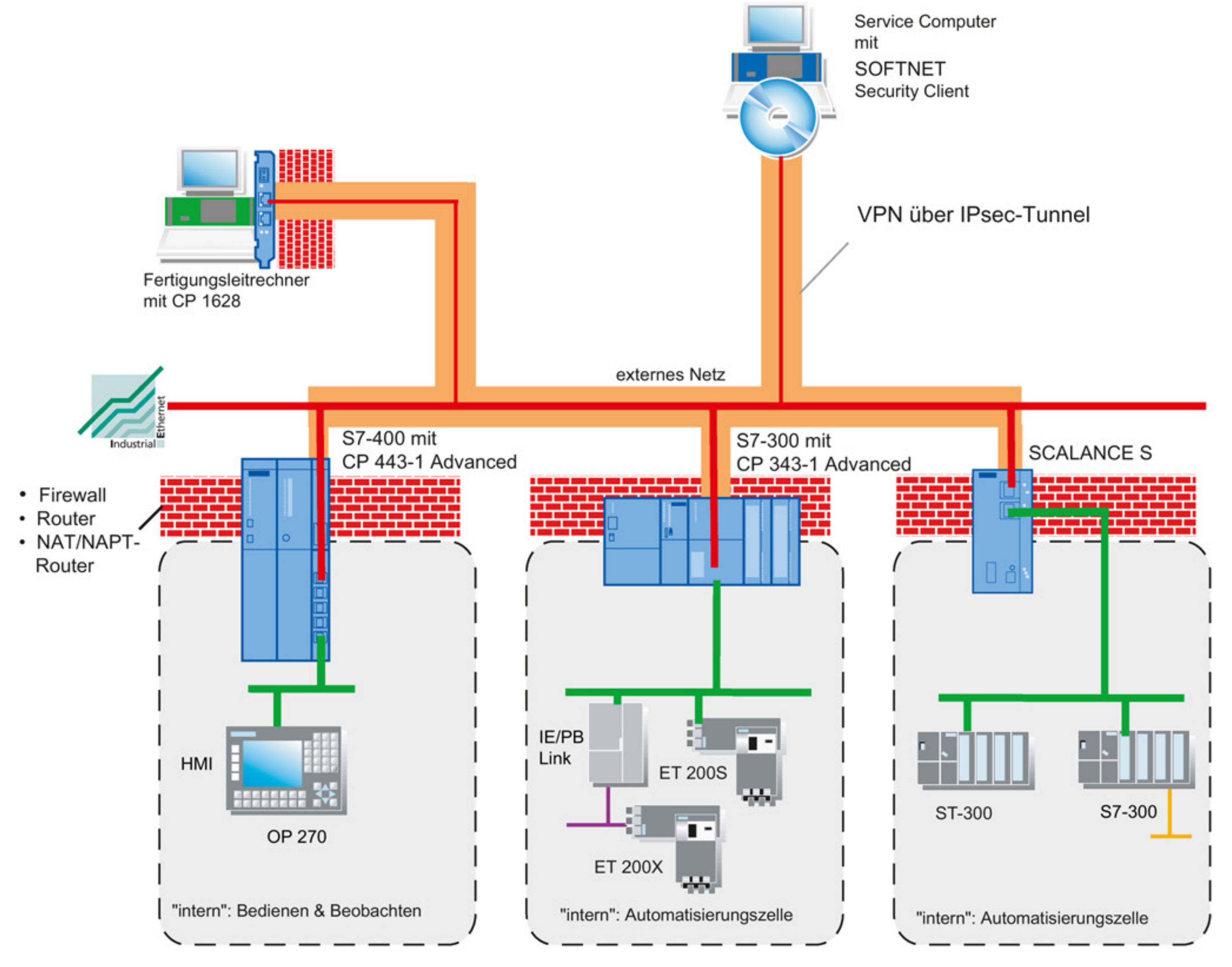


Bild 1-6 Netzkonfiguration mit CP x43-1 Adv.

Sicherheitsfunktionen

- Firewall
  - IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
  - Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3 (Layer 2)
  - Bandbreitenbegrenzung
  - Globale Firewall-Regelsätze

  Alle Netzknoten, die sich im internen Netzsegment eines CP x43-1 Adv. befinden, werden durch dessen Firewall geschützt.
- Gesicherte Kommunikation durch IPsec-Tunnel

  Der CP x43-1 Adv. kann mit anderen Security-Baugruppen per Projektierung zu Gruppen zusammengefasst werden. Zwischen allen Security-Baugruppen einer VPN-Gruppe werden IPsec-Tunnel aufgebaut (VPN). Alle internen Knoten dieser Security-Baugruppen können mittels dieser Tunnel gesichert miteinander kommunizieren.
- Logging

  Zur Überwachung lassen sich Ereignisse in Log-Dateien speichern, die mit Hilfe des Projektierwerkzeugs ausgelesen werden oder automatisch an einen Syslog-Server gesendet werden können.
- HTTPS

  Zur verschlüsselten Übertragung von Webseiten, z. B. bei der Prozesskontrolle.
- FTPS

  Zur verschlüsselten Übertragung von Dateien.
- NTP (gesichert)

  Zur sicheren Uhrzeitsynchronisierung und -übertragung.
- SNMPv3

  Zur abhörsicheren Übertragung von Netzwerkanalyseinformationen.
- Schutz für Geräte und Netzsegmente

  Die Schutzfunktion Firewall und VPN kann sich über den Betrieb einzelner Geräte, mehrerer Geräte wie auch ganzer Netzsegmente erstrecken.

Interne und Externe Netzknoten:

CP x43-1 Adv. teilt Netzwerke in zwei Bereiche auf:

- internes Netz: geschützte Bereiche mit den "internen Knoten"

  Interne Knoten sind alle diejenigen Knoten, die von einem CP x43-1 Adv. abgesichert sind.

- externes Netz: ungeschützte Bereiche mit den "externen Knoten"

  Externe Knoten sind alle Knoten, die sich außerhalb der geschützten Bereiche befinden.

Hinweis

Die internen Netze werden als sicher (vertrauenswürdig) betrachtet.

Verbinden Sie ein internes Netzsegment nur über CP x43-1 Adv. mit den externen Netzsegmenten.

Weitere Verbindungswege zwischen dem internen und externen Netz dürfen nicht vorhanden sein.

Informationen zu allgemeinen Funktionen des CP x43-1 Adv.

In dem vorliegenden Handbuch erhalten Sie Informationen zu den Security-Funktionen des CP x43-1 Adv. Für Beschreibungen zu allgemeinen Funktionen siehe:

- /1/ (Seite 278)
- /2/ (Seite 278)

1.10 Einsatz von CP 1628

Zellenschutzkonzept - Aufgabe von CP 1628

Die integrierten Sicherheitsmechanismen des CP 1628 ermöglichen die Absicherung von Rechnersystemen einschließlich der dazugehörigen Datenkommunikation innerhalb eines Automatisierungsnetzes oder den sicheren Fernzugriff über das Internet. Der CP 1628 erlaubt den Zugriff auf einzelne Geräte oder auch ganze Automatisierungszellen, die durch Security-Baugruppen geschützt sind und ermöglicht gesicherte Verbindungen über unsichere Netzwerkstrukturen.

Durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall und VPN (Virtual Private Network) über IPsec-Tunnel schützt der CP 1628 vor:

- Datenspionage
- Datenmanipulation
- unerwünschten Zugriffen

Die Security-Funktionen vom CP 1628 werden mit dem Projektierwerkzeug Security Configuration Tool konfiguriert, das in STEP 7 integriert ist.

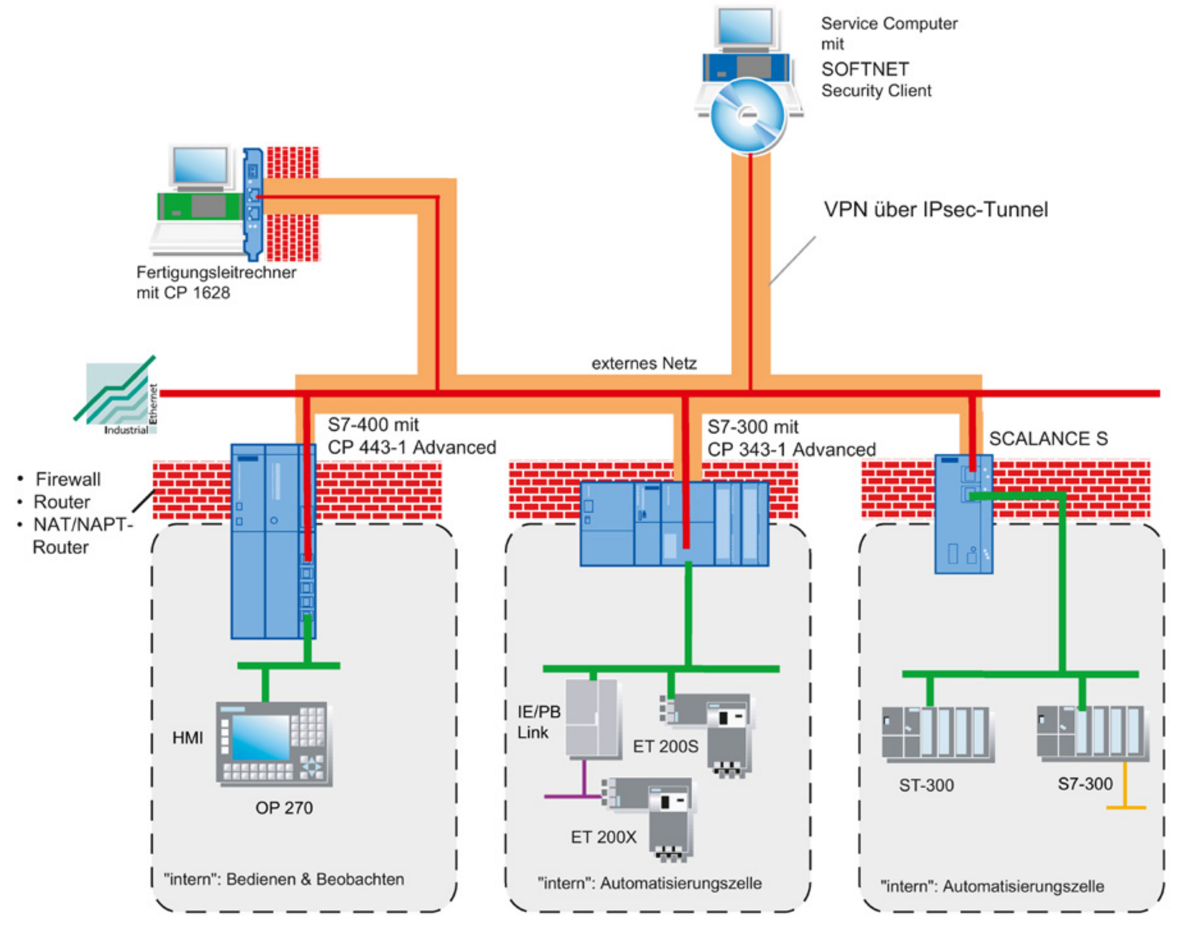


Bild 1-7 Netzkonfiguration mit CP 1628

Sicherheitsfunktionen

- Firewall
  - IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
  - Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3 (Layer 2)
  - Bandbreitenbegrenzung
  - Globale Firewall-Regeln
- Gesicherte Kommunikation durch IPsec-Tunnel

  Der CP 1628 kann mit anderen Security-Baugruppen per Projektierung zu Gruppen zusammengefasst werden. Zwischen allen Security-Baugruppen einer VPN-Gruppe werden IPsec-Tunnel aufgebaut (VPN, Virtual Private Network).
- Logging

  Zur Überwachung lassen sich Ereignisse in Log-Dateien speichern, die mit Hilfe des Projektierwerkzeugs ausgelesen werden oder automatisch an einen Syslog-Server gesendet werden können.
- NTP (gesichert)

  Zur sicheren Uhrzeitsynchronisierung und -übertragung.
- SNMPv3

  Zur abhörsicheren Übertragung von Netzwerkanalyseinformationen.

Informationen zu allgemeinen Funktionen des CP 1628

In dem vorliegenden Handbuch erhalten Sie Informationen zu den Security-Funktionen des CP 1628 erklärt. Für Beschreibungen zu allgemeinen Funktionen siehe

- /11/ (Seite 281)

1.11 Projektierung und Administration

Das Wichtigste zusammengefasst

Im Zusammenspiel mit dem Projektierwerkzeug Security Configuration Tool werden Sie zu einer einfachen und sicheren Anwendung der Security-Baugruppen geführt:

- Projektierung ohne IT-Experten-Wissen mit dem Security Configuration Tool

  Mit dem Security Configuration Tool können auch Nicht-IT-Experten eine Security-Baugruppe projektieren. Im Erweiterten Modus können bei Bedarf komplexere Einstellungen vorgenommen werden.

- Gesicherte administrative Kommunikation

  Die Übertragung der Einstellungen ist signiert und verschlüsselt und darf nur von autorisierten Personen durchgeführt werden.

- Zugriffsschutz im Security Configuration Tool

  Durch die Benutzerverwaltung des Security Configuration Tool ist ein Zugriffsschutz für die Security-Baugruppen und die Projektierdaten gewährleistet.

- Wechselmedium C-PLUG einsetzbar PC CP

  Der C-PLUG ist ein steckbares Wechselmedium, auf dem Konfigurationsdaten verschlüsselt abgespeichert sind. Er ermöglicht beim Austausch einer Security-Baugruppe die Konfiguration ohne PG/PC, sofern die Security-Baugruppe eine Datenhaltung auf dem C-PLUG unterstützt.

Projektierung mit Security Configuration Tool 2

Das Security Configuration Tool ist das zu den Security-Baugruppen mitgelieferte Projektierwerkzeug.

Das vorliegende Kapitel macht Sie mit der Bedienoberfläche und der Funktionsweise des Projektierwerkzeugs vertraut.

Sie erfahren, wie Security-Projekte eingerichtet, bedient und verwaltet werden.

Weitere Informationen

Wie Sie Security-Baugruppen und IPsec-Tunnel konfigurieren, wird ausführlich in den Folgekapiteln dieses Handbuchs erläutert.



Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe. Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

2.1 Übersicht - Leistungsumfang und Arbeitsweise

Leistungsumfang

Sie verwenden das Projektierwerkzeug Security Configuration Tool für diese Aufgaben:

- Projektierung der Security-Baugruppen
- Projektierung von SOFTNET Security Client
- Erstellen von VPN-Konfigurationsdaten für SCALANCE M
- Erstellen von VPN-Konfigurationsdateien für VPN-Geräte von Fremdherstellern
- Test- und Diagnosefunktionen, Statusanzeigen

Zwei Betriebsmodi des Security Configuration Tool

Das Security Configuration Tool kann in folgenden Betriebsmodi aufgerufen werden:

- Security Configuration Tool Standalone:
  - Kann unabhängig von STEP 7 aufgerufen werden
  - Keine Security-Projektierung von CPs möglich
- Security Configuration Tool in STEP 7 integriert:
  - Kann nur aus STEP 7 heraus aufgerufen werden
  - Mindestens ein CP mit aktivierter Security-Funktion muss sich im Projekt befinden
  - Der Umfang von Security Configuration Tool Standalone wird um die Möglichkeit, Security-Funktionen für CPs zu projektieren, erweitert

Offline-Projektierungssicht und Online-Diagnosesicht

Das Security Configuration Tool verfügt über eine Offline-Projektierungssicht und eine Online-Diagnosesicht:

- Offline-Projektierungssicht

  In der Betriebsart Offline erfolgt die Projektierung der Konfigurationsdaten für die entsprechende Baugruppe. Vor dem Ladevorgang muss hierbei keine Verbindung zu dieser Baugruppe bestehen.
- Online

  Der Online-Modus dient dem Test und der Diagnose einer Security-Baugruppe.

Zwei Bedienungsmodi

In der Offline-Projektierungssicht stellt das Security Configuration Tool zwei Bedienungsmodi zur Verfügung:

- Standard Modus

  Der Standard Modus ist im Security Configuration Tool voreingestellt. Dieser Modus ermöglicht eine zügige, unkomplizierte Projektierung für den Betrieb der Security-Baugruppen.
- Erweiterter Modus

  Im Erweiterten Modus gibt es erweiterte Einstellmöglichkeiten, die u.a. eine individuelle Einstellung der Firewall-Regeln, Log-Einstellungen, NAT-/NAPT-Regeln, VPN-Knoten sowie erweiterter Sicherheitsfunktionalitäten zulassen.

Arbeitsweise - Sicherheit und Konsistenz

- Zugriff nur für autorisierte Benutzer

  Jedes Projekt ist durch Benutzernamen- und Passwortvergabe vor unberechtigtem Zugriff geschützt. Mit Hilfe von Passwort-Richtlinien lassen sich projektspezifische Vorgaben für die Passwortvergabe definieren.
- Konsistente Projektdaten

  Schon während der Eingabe in den einzelnen Dialogen erfolgen Konsistenzprüfungen. Zusätzlich können Sie jederzeit eine dialogübergreifende projektweite Konsistenzprüfung durchführen.

  Auf die Security-Baugruppen können nur konsistente Projektdaten geladen werden.
- Schutz der Projektdaten durch Verschlüsselung

  Die Projekt- und Konfigurationsdaten sind in der Projektdatei und, sofern vorhanden, auch auf dem C-PLUG (nicht für CP 1628) durch Verschlüsselung geschützt.

2.2 Installation des Security Configuration Tools

2.2.1 Unterstützte Betriebssysteme

Unterstützte Betriebssysteme

Unterstützt werden die folgenden Betriebssysteme:

- Microsoft Windows XP 32 Bit + Service Pack 3
- Microsoft Windows 7 Professional 32/64 Bit
- Microsoft Windows 7 Professional 32/64 Bit + Service Pack 1
- Microsoft Windows 7 Ultimate 32/64 Bit
- Microsoft Windows 7 Ultimate 32/64 Bit + Service Pack 1
- Windows Server 2008 R2 64 Bit
- Windows Server 2008 R2 64 Bit + Service Pack 1

Hinweis

Vor der Installation des Security Configuration Tool lesen Sie unbedingt die auf der DVD mitgelieferte Datei "LIESMICH.htm". In dieser Datei sind ggf. wichtige Hinweise und die letzten Änderungen vermerkt.

SCALANCE S - Gehen Sie so vor

Sie installieren das Projektierwerkzeug Security Configuration Tool von der mitgelieferten Produkt-DVD.

- Legen Sie die Produkt-DVD in Ihr DVD-ROM-Laufwerk. Bei eingeschalteter Autorun-Funktion wird die Oberfläche automatisch gestartet, von der aus Sie die Installation durchführen können.

oder

- Starten Sie die auf der mitgelieferten Produkt-DVD vorhandene Anwendung "start.exe".

CP x43-1 Adv. - Gehen Sie so vor

Sie installieren das Projektierwerkzeug Security Configuration Tool von dem STEP 7 Datenträger. Sie finden die Installationsdatei auf dem STEP 7 Datenträger im Verzeichnis für optionale Softwarekomponenten.

CP 1628 - Gehen Sie so vor

Sie installieren das Projektierwerkzeug Security Configuration Tool von dem mitgelieferten Datenträger, der die Treiberdaten des CP 1628 enthält.

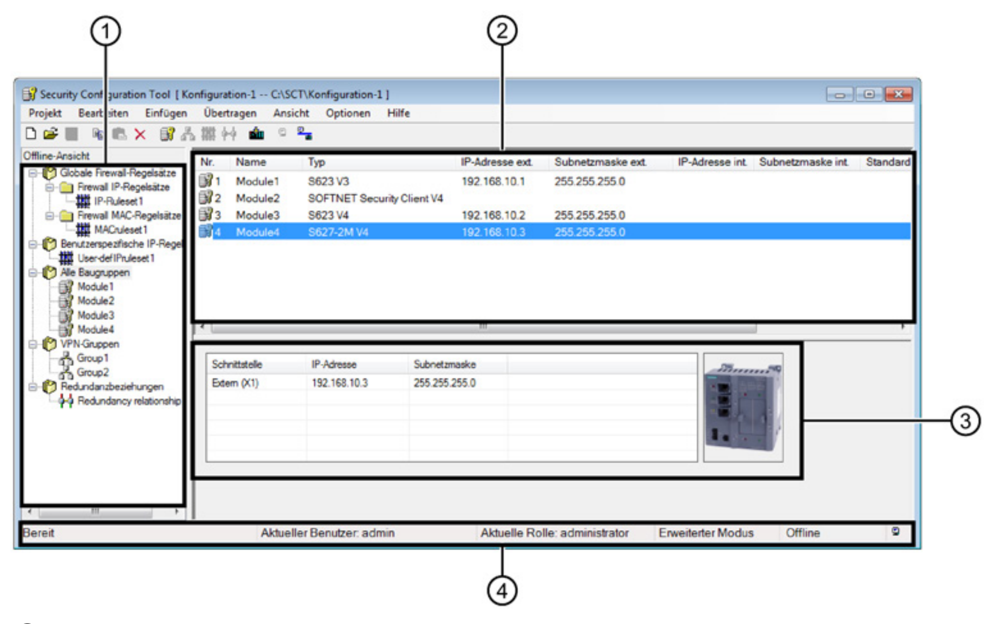
- Legen Sie den Datenträger in Ihr DVD-ROM-Laufwerk. Bei eingeschalteter Autorun-Funktion wird die Oberfläche automatisch gestartet, von der aus Sie die Installation durchführen können.

oder

- Starten Sie die auf dem mitgelieferten Datenträger vorhandene Anwendung "setup.exe".

2.3 Bedienoberfläche und Menübefehle

Aufbau der Bedienoberfläche im Erweiterten Modus



① Navigationsbereich:

- Globale Firewall-Regelsätze

  Das Objekt enthält die projektierten globalen Firewall-Regelsätze. Weitere Ordner unterscheiden nach:

  – Firewall IP-Regelsätzen
  – Firewall MAC-Regelsätzen

- Benutzerspezifische IP-Regelsätze S≥V3.0
- Alle Baugruppen

  Das Objekt enthält alle projektierten Baugruppen und SOFTNET Konfigurationen des Projekts.

- VPN-Gruppen

  Das Objekt enthält alle erzeugten VPN-Gruppen.

- Redundanzbeziehungen S≥V4.0

  Das Objekt enthält alle erzeugten Redundanzbeziehungen des Projekts.

② Inhaltsbereich:

Indem Sie ein Objekt im Navigationsbereich anwählen, erhalten Sie im Inhaltsbereich Detailinformationen zu diesem Objekt.

Für einige Security-Baugruppen können Sie in diesem Bereich Auszüge der Schnittstellen-Konfigurationen einsehen und anpassen.

Durch Doppelklick auf die Security-Baugruppen werden, sofern diese die entsprechenden Konfigurationsmöglichkeiten bieten, Eigenschaftsdialoge zur Eingabe weiterer Parameter geöffnet.

③ Detail-Fenster:

Das Detail-Fenster enthält zusätzliche Informationen zum ausgewählten Objekt und ermöglicht im jeweiligen Kontext einer VPN-Gruppe die Projektierung verbindungsgranularer VPN-Eigenschaften.

Das Detail-Fenster kann über das Menü "Ansicht" aus- und eingeblendet werden.

④ Statuszeile:

Die Statuszeile zeigt Bedienzustände und aktuelle Statusmeldungen an. Hierzu gehören:

- Der aktuelle Benutzer und der Benutzertyp
- Die Bedienungssicht - Standard Modus / Erweiterter Modus
- Die Betriebsart - Online / Offline

Symbolleiste

Nachfolgend eine Übersicht der wählbaren Symbole in der Symbolleiste und deren Bedeutung.

Symbol	Bedeutung / Bemerkungen
	Neues Projekt anlegen.
	Bestehendes Projekt öffnen.
	Geöffnetes Projekt unter aktuellem Pfad und Projektnamen speichern.
	Angewähltes Objekt kopieren.
	Objekt aus der Zwischenablage einfügen.
	Angewähltes Objekt löschen.
	Neue Baugruppe anlegen. Das Symbol ist nur aktiv, wenn Sie sich innerhalb des Navigationsbereichs im Ordner "Alle Baugruppen" befinden.
	Neue VPN-Gruppe anlegen. Das Symbol ist nur aktiv, wenn Sie sich innerhalb des Navigationsbereichs im Ordner "VPN-Gruppen" befinden.
	Einen neuen globalen IP-Regelsatz / MAC-Regelsatz oder benutzerspezifischen IP-Regelsatz anlegen. Das Symbol ist nur aktiv, wenn Sie sich innerhalb des Navigationsbereichs in einem Unterordner von "Globale Firewall-Regelsätze" oder auf dem Ordner "Benutzerspezifische IP-Regelsätze" befinden.
	Neue Redundanzbeziehung anlegen. Das Symbol ist nur aktiv, wenn Sie sich innerhalb des Navigationsbereichs im Ordner "Redundanzbeziehungen" befinden.

Symbol	Bedeutung / Bemerkungen
	Konfiguration in die selektierten Security-Baugruppen laden bzw. Konfigurationsdaten für SOFTNET Security Client / SCALANCE M / VPN-Gerät / NCP VPN-Client (Android) er-stellen.
	In den Offline-Modus umschalten.
	In den Online-Modus umschalten.

Menüleiste

Nachfolgend eine Übersicht der wählbaren Menübefehle und deren Bedeutung.

Menübefehl		**Bedeutung / Bemerkungen**	**Tastenkombination**
Projekt ▸…		Funktionen für die projektspezifischen Einstellungen sowie das Laden und Speichern der Projektdatei.	
	Neu...	Neues Projekt anlegen. Für CP: Projekte werden durch STEP 7-Projektierung angelegt.	
	Öffnen...	Bestehendes Projekt öffnen. Für CP: Bestehende Projekte können nur über STEP 7-Projekte geöffnet werden.	
	Speichern	Geöffnetes Projekt unter aktuellem Pfad und Projektnamen speichern.	Strg + S
	Speichern unter...	Geöffnetes Projekt unter wählbarem Pfad und Projektnamen speichern. Für CP: Das Projekt ist Teil des STEP 7-Projekts. Der Pfad kann nicht geändert werden.	
	Eigenschaften...	Dialog für Projekteigenschaften öffnen.	
	Zuletzt geöffnete Projekte	Direkte Auswahlmöglichkeit der bisher bearbeiteten Projekte. Für CP: Bestehende Projekte können nur über STEP 7 geöffnet werden.	
	Beenden	Projekt schließen.	
Bearbeiten ▸…		Menübefehle nur im Offline-Modus **Hinweis** Die Funktionen können Sie bei angewähltem Objekt teilweise auch über das Kontextmenü auswählen.	
	Kopieren	Angewähltes Objekt kopieren.	Strg + C
	Einfügen	Objekt aus der Zwischenablage holen und einfügen.	Strg + V
	Löschen	Angewähltes Objekt löschen.	Entf
	Umbenennen	Angewähltes Objekt umbenennen.	F2
	Neues Zertifikat...	Neues Gruppenzertifikat für Baugruppe erzeugen, die nach Auswahl der zugehörigen VPN-Gruppe im Inhaltsbereich selektiert wurde.	
	Baugruppe austauschen ...	Angewählte Security-Baugruppe durch eine andere austauschen.	
	Eigenschaften ...	Eigenschaftsdialog des angewählten Objektes öffnen.	F4
	Online-Diagnose ...	Auf die Test- und Diagnosefunktionen zugreifen.	
Einfügen ▸…		Menübefehle nur im Offline-Modus	
	Baugruppe	Neue Security-Baugruppe anlegen. Der Menübefehl ist nur aktiv, wenn eine Security-Baugruppe oder eine VPN-Gruppe im Navigationsbereich angewählt ist.	Strg + M

Menübefehl		Bedeutung / Bemerkungen	Tastenkombination
	Gruppe	Neue VPN-Gruppe anlegen. Der Menübefehl ist nur aktiv, wenn ein Gruppen-Objekt im Navigationsbereich angewählt ist.	Strg + G
	Firewall-Regelsatz	Einen neuen globalen Firewall IP-Regelsatz, MAC-Regelsatz oder benutzerspezifischen IP-Regelsatz anlegen. Der Menübefehl ist nur aktiv, wenn ein Firewall-Objekt im Navigationsbereich angewählt ist. Der Menübefehl ist nur im Erweiterten Modus sichtbar.	Strg + F
	Redundanzbeziehung	Neue Redundanzbeziehung anlegen. Der Menübefehl ist nur aktiv, wenn Sie sich innerhalb des Navigationsbereichs im Ordner "Redundanzbeziehungen" befinden.	Strg + R
Übertragen ▸…			
	An Baugruppe(n)...	Konfiguration auf die selektierte(n) Security-Baugruppe(n) laden bzw. Konfigurationsdaten für SOFTNET Security Client / SCALANCE M / VPN-Geräte / NCP VPN-Clients (Android) erstellen. Anmerkung: Es können nur konsistente Projektdaten geladen werden. Für CPs: Projektdaten können nur über STEP 7 geladen werden.	
	An alle Baugruppen...	Konfiguration auf alle Security-Baugruppen laden. Anmerkung: Es können nur konsistente Projektdaten geladen werden.	
	Konfigurationszustand...	Konfigurationszustand der projektierten Security-Baugruppen wird in einer Liste anzeigt.	
	Firmware übertragen ...	Neue Firmware in selektierte Security-Baugruppe laden. Für S7-CPs: Die Firmware wird über das Aktualisierungs-Zentrum der Web-Diagnose auf den CP geladen.	
Ansicht ▸…			
	Erweiterter Modus	Vom Standard Modus (Voreinstellung) in den Erweiterten Modus umschalten. **Achtung** Sie können eine einmal vorgenommene Umschaltung in den Erweiterten Modus für das aktuelle Projekt nicht mehr rückgängig machen.	Strg + E
	Detail-Fenster einblenden	Zusätzliche Details zum ausgewählten Objekt ein- und ausblenden.	Strg + Alt + D
	Offline	Voreinstellung. Umschaltung in die Offline-Projektierungssicht.	Strg + Shift + D
	Online	Umschaltung in die Online-Diagnosesicht.	Strg + D

Menübefehl		Bedeutung / Bemerkungen	Tastenkombination
Optionen ▸…			
	IP-Dienste...	Dialog für Dienst-Definitionen für IP-Firewall-Regeln öffnen. Der Menübefehl ist nur im Erweiterten Modus sichtbar.	
	MAC-Dienste...	Dialog für Dienst-Definitionen für MAC-Firewall-Regeln öffnen. Der Menübefehl ist nur im Erweiterten Modus sichtbar.	
	Netzwerkadapter...	Über den ausgewählten Netzwerkadapter wird dem SCALANCE S eine IP-Adresse zugewiesen.	
	Sprache...	Sprache auswählen, in der die SCT-Oberfläche angezeigt wird. Für SCT in STEP 7 wird die Sprache der SCT-Oberfläche über die Sprachauswahl in STEP 7 festgelegt.	
	Log-Dateien...	Anzeige von gespeicherten Log-Dateien.	
	Symbolische Namen...	Symbolische Namen für IP- oder MAC-Adressen vergeben.	
	Konfiguration der NTP-Server...	NTP-Server erstellen und bearbeiten.	
	Konfiguration der RADIUS-Server...	RADIUS-Server erstellen und bearbeiten.	
	Konsistenzprüfungen...	Konsistenz des gesamten Projektes prüfen. Als Ergebnis wird eine Resultatsliste ausgegeben.	
	Benutzerverwaltung...	Benutzer und Rollen anlegen und bearbeiten, Rechte zuweisen und Passwort-Richtlinien definieren.	
	Zertifikatsmanager...	Zertifikate anzeigen oder importieren / exportieren.	
Hilfe ▸…			
	Hilfethemen...	Hilfe zu den Funktionen und Parametern, die Sie im SCT vorfinden.	F1
	Info...	Informationen zum Versions- und Ausgabestand des SCT.	

2.4 Projekte anlegen und verwalten

2.4.1 Security Configuration Tool (Standalone-Variante)



Projektierung mit dem Security Configuration Tool Standalone

Das Security Configuration Tool Standalone wird für die Erstellung von Security-Projekten verwendet, in welchen keine Security-Baugruppen projektiert werden, die in STEP 7 erstellt und konfiguriert werden müssen.

Über den Menübefehl "Projekt" > "Neu…" legen Sie ein neues Projekt an. Dieses umfasst sämtliche Konfigurations- und Verwaltungsinformationen für ein oder mehrere SCALANCE S, SOFTNET Security Clients, SCALANCE M-Geräte, VPN-Geräte sowie NCP VPN-Clients (Android). Für jedes Gerät bzw. für jede Konfiguration legen Sie im Projekt eine Baugruppe an.

2.4.2 Security Configuration Tool in STEP 7

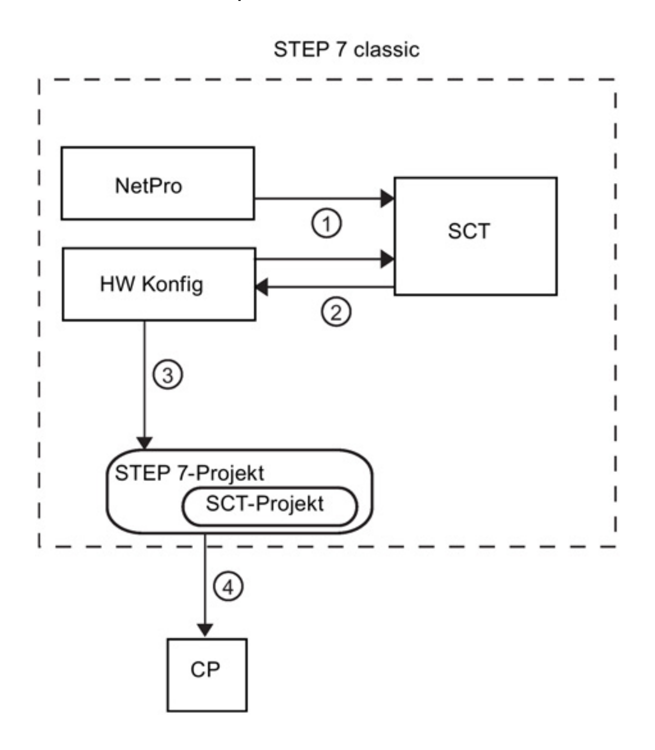
Projektierung

Das Security Configuration Tool in STEP 7 wird für die Erstellung von Security-Projekten verwendet, in welchen Security-Baugruppen projektiert werden, die in STEP 7 erstellt und konfiguriert werden müssen. Zusätzlich werden alle Security-Baugruppen der Standalone-Variante unterstützt.

Sobald Sie in STEP 7 für eine Security-Baugruppe die Security-Funktion aktivieren, wird automatisch ein SCT-Projekt angelegt, in welchem die Daten der Security-Konfiguration abgelegt und verwaltet werden. Sämtliche Daten zur Security-Konfiguration werden intern von SCT bearbeitet und das Ergebnis an STEP 7 zurückgeliefert.

Zusammenspiel von STEP 7 und SCT

Das Zusammenspiel von STEP 7 und SCT wird anhand der folgenden Darstellung erläutert:



① Nehmen Sie über STEP 7 Security-Einstellungen vor, wird SCT aufgerufen, da dort die Daten für Security gepflegt und verwaltet werden.

Sind in NetPro spezifizierte Verbindungen projektiert, werden für diese nach dem Speichern und Übersetzen automatisch Firewall-Regeln in SCT angelegt.

② In SCT nehmen Sie weitere Security-Einstellungen vor. SCT bearbeitet die Daten intern und gibt das Ergebnis an STEP 7 zurück.

③ Aktionen wie "Speichern Unter" und "Übersetzen" finden innerhalb von STEP 7 statt. Die Security-Daten werden als SCT-Projekt unter einem automatisch vergebenen Namen in einem Unterordner des STEP 7-Projektes gespeichert. Name und Speicherort dürfen nicht verändert werden. Für ein STEP 7-Projekt kann genau ein SCT-Projekt angelegt werden. Ein mit dem Security Configuration Tool in STEP 7 angelegtes SCT-Projekt kann nicht mit dem Security Configuration Tool im Standalone-Modus geöffnet werden.

④ Die projektierten Security-Daten des CP werden über STEP 7 auf die Baugruppe geladen.

Welche Daten werden von STEP 7 nach SCT migriert und im Inhaltsbereich angezeigt?

Folgende in STEP 7 angelegte Projektierungsdaten werden automatisch von SCT übernommen, können dort jedoch nicht verändert werden:

- Gerätename
- IP-Adresse PROFINET-IO ~~PC CP~~

- IP-Adresse GBit
- Subnetzmaske PROFINET-IO
- Subnetzmaske GBit
- MAC-Adresse der GBit-Schnittstelle
- Standard-Router
- MAC-Adresse PROFINET-IO

Welche Daten können nach SCT migriert und dort verändert werden?

Folgende in STEP 7 genutzte Funktionen können nach SCT migriert und dort bearbeitet werden:

- Access Control-Listen (Seite 121)
- Benutzer (Seite 67)
- NTP-Server (Seite 193)



Detailinformationen dazu finden Sie in der Online-Hilfe von SCT.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen SCT-Dialog.

Automatische Firewall-Regeln für projektierte Verbindungen

Für in STEP 7 projektierte spezifizierte Verbindungen werden automatisch Firewall-Regeln in SCT angelegt, die den Verbindungsaufbau freigeben. Nähere Informationen hierzu finden Sie im folgenden Kapitel:

- Verbindungsbezogene automatische Firewall-Regeln (Seite 146).

Für unspezifizierte Verbindungen müssen Sie die Firewall-Regeln, die den Verbindungsaufbau freigeben, in SCT konfigurieren. Nähere Informationen hierzu finden Sie im folgenden Kapitel:

- Firewall im Erweiterten Modus (Seite 139).

Security-Einstellungen in STEP 7 vornehmen

Security-Einstellungen nehmen Sie wie folgt vor:

- Über einzelne Register der Objekteigenschaften

  In einzelnen Registern können Sie CP-spezifische Security-Funktionen aktivieren und ausführen. Beim Ausführen wird der entsprechende SCT-Dialog geöffnet, in dem Sie Security-Einstellungen vornehmen können. In folgenden Registern können Sie Security-Einstellungen vornehmen:

	Register	Funktion	Beschreibung
	Security	Security aktivieren	• Die Security-Funktionen in den einzelnen Registern werden aktiv. • Das Menü "Bearbeiten" > "Security Configuration Tool" wird aktiv, über welches Sie das Security Configuration Tool öffnen. Dort können Sie weitere, Security-Baugruppen übergreifende Einstellungen vornehmen, wie z. B. VPN-Gruppen anlegen oder Security-Baugruppen hinzufügen, die nicht in STEP 7 projektierbar sind. • Falls Sie für die Security-Baugruppe Benutzer in STEP 7 projektiert haben, öffnet sich das Fenster " Datenmigration für securityrelevante Projektdaten", über das Sie die STEP 7 Benutzer in das Security Configuration Tool migrieren können.
		Start der Security-Konfiguration	SCT öffnet sich in einem Übersichtmodus, in dem Sie die für diese Security-Baugruppe spezifischen Eigenschaften konfigurieren können.
		Firewall-Regeln online nachladen	Angepasste Firewall-Einstellungen werden generiert und auf den CP geladen, ohne ein Stoppen des CP zu verursachen.
		Firewall-Regeln online nachladen (CP 1628)	Angepasste Firewall-Einstellungen werden generiert und auf den CP geladen.
	Benutzer	Start der Benutzerverwaltung	Startet die SCT-Benutzerverwaltung, in der Benutzer und Rollen angelegt sowie Rechte zugewiesen werden.
PC CP	IP-Zugriffsschutz	Start der Firewall-Konfiguration	Beim Aktivieren von Security wird eine vorhandene IP-Zugriffsliste über eine Umsetzung in Firewall-Regeln in das Security Configuration Tool migriert.
	FTP	Zugriff nur über FTPS zulassen	Startet die SCT-Benutzerwaltung, in der Sie einer Rolle FTP-Rechte zuweisen können.
		Start der Benutzerverwaltung	
	Web	Zugriff nur über HTTPS zulassen	Startet die SCT-Benutzerwaltung, in der Sie einer Rolle Web-Rechte zuweisen können.
		Start der Benutzerverwaltung	
	Uhrzeitsynchronisation	Erweiterte NTP-Konfiguration	Startet das SCT im NTP-Konfigurationsmodus.
	SNMP	Start der SNMP-Konfiguration	Startet SCT im SNMP-Konfigurationmodus. Sie können zwischen SNMPv1 oder SNMPv3 wählen.
		Start der Benutzerverwaltung	Startet die SCT-Benutzerwaltung, in der Sie einer Rolle SNMP-Rechte zuweisen können.

- Direkt in SCT

Sie rufen SCT in STEP 7 über das Menü "Bearbeiten" > "Security Configuration Tool" auf. Zusätzlich zu den Einstellungen in den Registern der Objekteigenschaften legen Sie hier z. B. VPN-Gruppen an oder fügen SCALANCE S-Baugruppen hinzu. Die SCALANCE S-Baugruppen können Sie in SCT zwar projektieren und laden, die Daten werden jedoch nicht an STEP 7 zurückgeliefert. Auch werden die Baugruppen nach Beendigung des SCT nicht in STEP 7 angezeigt.

Hinweis

Nähere Angaben finden Sie in der STEP 7 Online-Hilfe sowie in der SCT Online-Hilfe.

Allgemeine Informationen zu STEP 7 finden Sie in /9/ (Seite 280).

2.4.3 STEP 7-Daten migrieren

STEP 7-Gerätebenutzer in die SCT-Benutzerverwaltung migrieren

Wählen Sie in dem Migrationsdialog aus, wie die in STEP 7 angelegten Benutzer in die SCT-Benutzerverwaltung migriert werden sollen. Dabei stehen Ihnen folgende Aktionen zur Auswahl:

Aktion	Beschreibung
Übernehmen als…	Der Benutzer wird unter einem anderen Namen in die SCT-Benutzerverwaltung migriert. Geben Sie den Namen in die Spalte "Migrierter Benutzername" ein. Dem migrierten Benutzer wird in SCT eine automatisch generierte Rolle zugewiesen.
Zusammenführen	Ist im SCT-Projekt bereits ein Benutzer mit dem gleichen Namen angelegt, werden die beiden Benutzer zusammengelegt. Die Rolle des SCT-Benutzers wird um die ausgewählten Rechte des migrierten Benutzers erweitert.
Nicht übernehmen	Der Benutzer der Security-Baugruppe wird nicht in die SCT-Benutzerverwaltung migriert. Eine nachträgliche Migration ist nicht möglich.

Hinweis

Folgende Daten werden nicht migriert

- Passwörter bereits angelegter Benutzer in STEP 7. Wählen Sie deshalb für jeden Benutzer aus, wie er migriert werden soll und vergeben Sie über die Schaltfläche "Passwort vergeben" ein neues Passwort.
- Der in STEP 7 verfügbare systemdefinierte Benutzer "everybody". Auch werden dessen Rechte für migrierte Benutzer nicht übernommen.

Hinweis

Die Benutzer und deren Rollen können nach der Migration in der Benutzerverwaltung des Security Configuration Tools angepasst werden.

STEP 7-Geräterechte in die SCT-Benutzerverwaltung migrieren

Folgende Rechte werden migriert:

Recht in STEP 7	Recht nach der Migration in SCT	Service
Auf die projektierten Symbole zuzugreifen	Applet: Variablen über projektierte Symbole lesen	SPS
	Applet: Variablen über projektierte Symbole schreiben	
Variablen über absolute Adressen zu lesen	Applet: Variablen über absolute Adressen lesen	
Variablen über absolute Adresse zu schreiben	Applet: Variablen über absolute Adressen schreiben	
Mit FTP auf Dateien in der S7-Station zugreifen	FTP: Dateien (DBs) von der S7-CPU lesen	
	FTP: Dateien (DBs) in die S7-CPU schreiben	
	FTP: Dateien vom CP-Dateisystem lesen	Dateisystem
	FTP: Dateien auf das CP-Dateisystem schreiben	
	Web: CP-Dateisystem formatieren	
Eine Testmail über die Systemseite zu versenden	Web: Auf Web-Diagnose und CP-Dateisystem zugreifen	Web
	Web: Testmail versenden	
Den Status von Baugruppen abzufragen	Applet: Status der Baugruppen im Rack lesen	SPS
Die Bestellnummer von Baugruppen abzufragen	Applet: Bestellnummer der Baugruppen im Rack lesen	

Siehe auch

Zeitsynchronisierung (Seite 193)

Zugriffsliste projektieren (Seite 121)

2.4.4 Übersicht

Allgemeine Inhalte

Sowohl in der Standalone-Version des Security Configuration Tools als auch in der in STEP 7 integrierten Version werden Sie beim Anlegen eines neuen Projektes aufgefordert, einen Benutzernamen und ein Passwort zu vergeben. Der Benutzer, den Sie hier anlegen, ist vom Typ "administrator". Nach der Eingabe können Sie die Konfigurationen im Projekt vornehmen.

Allgemein beinhalten die Konfigurationen eines Projektes:

- Projektweit gültige Einstellungen
- Baugruppenspezifische Einstellungen
- Gruppenzuordnungen für IPsec-Tunnel S602

Zusätzlich regelt eine Benutzerverwaltung die Zugriffsberechtigungen auf die Projektdaten und auf die Security-Baugruppen.

Projektweit gültige Einstellungen

- Projekteigenschaften

  Diese umfassen neben allgemeinen Adress- und Namensangaben Vorgaben für Initialisierungswerte.
- Globale Firewall-Regelsätze

  Ein globaler Firewall-Regelsatz kann mehreren Security-Baugruppen gleichzeitig zugewiesen werden. Diese Möglichkeit vereinfacht in vielen Fällen die Projektierung im Gegensatz zur Projektierung von lokalen Firewall-Regeln in den baugruppenspezifischen Einstellungen.
- Benutzerspezifische IP-Regelsätze S≥V3.0

  Ein benutzerspezifischer IP-Regelsatz wird einem Benutzer und einer Security-Baugruppe zugewiesen. Einer SCALANCE S V4 Baugruppe kann auch ein benutzerspezifischer IP-Regelsatz zugewiesen werden, welchem eine Rolle zugeordnet ist.

  Benutzerspezifische IP-Regelsätze ermöglichen die Definition von feingranularen, benutzerspezifischen Zugriffsrechten.
- Redundanzbeziehungen S62x ≥ V4.0

  Eine Redundanzbeziehung wird für zwei Security-Baugruppen angelegt. Wenn eine der beiden Security-Baugruppen im Betrieb ausfällt, übernimmt die andere Security-Baugruppe deren Funktion als Firewall und (NAT-/NAPT-)Router.
- MRP-Domains S627-2M

  Mit Hilfe von MRP-Domains werden die Teilnehmer eines MRP-Rings festgelegt. Für die Schnittstellen aller Baugruppen, die an einen MRP-Ring angebunden sein sollen, muss dieselbe MRP-Domain ausgewählt sein.

- Dienst-Definitionen

  Mithilfe der Definition von IP- oder MAC-Diensten können Sie Firewall-Regeln kompakt und übersichtlich definieren.

- NTP-Server

  NTP-Server werden projektweit angelegt und können dann in SCT mehreren Security-Baugruppen zugewiesen werden.

- RADIUS-Server S≥V4.0

  RADIUS-Server werden projektweit angelegt und können dann in SCT mehreren Security-Baugruppen zugewiesen werden.

- Zertifikatsmanager

  Im Zertifikatsmanager werden sämtliche Zertifikate des Projektes und der darin enthaltenen Security-Baugruppen verwaltet.

- Benutzerverwaltung

  In der Benutzerverwaltung können Sie alle Benutzer des Projektes und deren Rechte verwalten sowie Passwortrichtlinien definieren.

- Symbolische Namen

  In einem Projekt können Sie stellvertretend für IP- und MAC-Adressen symbolische Namen in einer Tabelle vergeben.

Baugruppenspezifische Einstellungen

Die meisten Funktionen werden in den Registern des Eigenschaftsdialogs konfiguriert, welcher für eine selektierte Security-Baugruppe über den Menübefehl "Bearbeiten" > "Eigenschaften..." aufgerufen werden kann. Im Eigenschaftsdialog können die einzelnen Register per Drag & Drop beliebig angeordnet werden. In der folgenden Tabelle sind die Funktionsbeschreibungen der einzelnen Register dargestellt.

	Funktion / Register im Eigenschaftendialog	**wird angeboten im Modus ...**	
		Standard	**Erweiterter**
	Schnittstellen Übersicht der einzelnen Schnittstellen- und Porteinstellungen. Für CPs: Die Einstellungen werden aus STEP 7 übernommen und können nicht verändert werden.	X	X
	Firewall Im Standard Modus aktivieren Sie hier die Firewall mit einfachen Standard-Regeln. Zusätzlich können Sie Log-Einstellungen aktivieren. Im Erweiterten Modus können Sie detaillierte Paketfilter-Regeln definieren. Außerdem können Sie für jede Paketfilter-Regel explizite Log-Einstellungen definieren. Für CPs: Falls eine Access Control-Liste migriert wurde, wird diese hier angezeigt und kann bearbeitet werden.	X	X
S≥V3.0	**Internetverbindung** Wenn eine Verbindung über PPPoE eingestellt ist, nehmen Sie hier Einstellungen zum Internet Service Provider vor.	X	X
S≥V3.0	**DNS** Einstellungen zu dynamischem DNS, die den Zugriff auf sich ständig ändernde IP-Adressen über fest definierte Namen (FQDN) erlauben. Dynamisches DNS ist auf der externen Schnittstelle und auf der DMZ-Schnittstelle zugelassen.	-	X
~~SP~~	**Routing** Geben Sie hier die Daten zum Standard-Router ein und/oder legen Sie eine subnetzspezifische Route fest. Für CPs: Die Angabe eines Standard-Routers wird aus STEP 7 übernommen und kann auch nur dort verändert werden. Die Anzeige erfolgt im Inhaltsbereich von SCT. Das Register ist in den Moduleigenschaften daher nicht vorhanden.	X	X
~~PC CP~~	**NAT/NAPT** Aktivieren Sie die NAT-/NAPT-Funktionalität und legen Sie in einer Liste die Adressumsetzung fest.	-	X
	Zeitsynchronisierung Legen Sie hier die Synchronisationsart für Datum und Uhrzeit fest. Für CPs: Die Zeitsynchronisierung kann in SCT nur dann konfiguriert werden, wenn in STEP 7 die erweiterte NTP-Konfiguration aktiviert wurde.	X	X

	Funktion / Register im Eigenschaftendialog	wird angeboten im Modus ...	
		Standard	Erweiterter
	Log-Einstellungen Sie können hier genauere Angaben zum Aufzeichnungs- und Speichermodus von Log-Ereignissen treffen und die Übertragung zu einem Syslog-Server projektieren.	-	X
S602	**VPN** Befindet sich die Security-Baugruppe in einer VPN-Gruppe, können Sie hier die Dead-Peer-Detection, die Art des Verbindungsaufbaus und ggf. einen WAN-Zugangspunkt (IP-Adresse oder FQDN) konfigurieren. Im Dialogbereich "VPN-Knoten" nehmen Sie zusätzlich je nach Security-Baugruppe Einstellungen zu Subnetzen, IP-/MAC-Knoten und NDIS-Knoten vor, welche zusätzlich über die VPN-Tunnel erreicht werden sollen. Für SCALANCE S: Das Lernen von internen Knoten kann aktiviert oder deaktiviert werden. Der Dialogbereich "VPN-Knoten" wird nur angezeigt, wenn sich das Projekt im Erweiterten Modus befindet.	X	X
SC	**DHCP-Server** Für das interne Netz sowie für das DMZ-Netz (nur SCALANCE S623/S627-2M) können Sie die Security-Baugruppe als DHCP-Server verwenden.	-	X
	SNMP Stellen Sie in diesem Register die SNMP-Protokollversion und das Authentifizierungs-/Verschlüsselungsverfahren ein.	X	X
S≥V3.0	**Proxy-ARP** Stellen Sie in diesem Register statische Einträge für Proxy-ARP auf der externen Schnittstelle ein.	-	X
S627-2M	**MRP/HRP** Stellen Sie in diesem Register die Parameter zur Anbindung der Security-Baugruppe an MRP-/HRP-Ringe ein.	X	X
S≥V4.0	**RADIUS** Weisen Sie der Security-Baugruppe in diesem Register einen RADIUS-Server zu, der Benutzer bei der Aktivierung benutzerspezifischer IP-Regelsätze anstelle der Security-Baugruppe authentifiziert.	X	X

Gruppenzuordnungen für VPN-Tunnel



VPN-Gruppen legen fest, welche Security-Baugruppen, SOFTNET Security Clients, SCALANCE M Baugruppen, VPN-Geräte und NCP VPN-Clients (Android) miteinander über IPsec-Tunnel kommunizieren sollen.

Indem Sie diese Netzwerkteilnehmer einer VPN-Gruppe zuordnen, können sie über ein VPN (Virtual Private Network) Kommunikationstunnel aufbauen.

Nur Baugruppen der gleichen VPN-Gruppe können untereinander gesichert über Tunnel kommunizieren, wobei die Baugruppen mehreren VPN-Gruppen gleichzeitig angehören können.

Siehe auch

Weitere Baugruppeneigenschaften projektieren (Seite 171)

2.4.5 Standard-Initialisierungswerte für ein Projekt festlegen



Standard-Initialisierungswerte für ein Projekt festlegen

Mit den Standard-Initialisierungswerten legen Sie Eigenschaften fest, die beim Anlegen neuer Baugruppen automatisch übernommen werden. Über das Kontrollkästchen "Auswahl speichern" legen Sie außerdem fest, ob beim Anlegen einer neuen Baugruppe ein Fenster zum Einstellen der Eigenschaften geöffnet werden soll oder ob die Baugruppe direkt eingefügt wird.

Wählen Sie den Menübefehl "Projekt" > "Eigenschaften…", Register "Standard-Initialisierungswerte".

Schutz der Projektdaten durch Verschlüsselung

Die abgespeicherten Projekt- und Konfigurationsdaten sind sowohl in der Projektdatei als auch auf dem C-PLUG (nicht für CP 1628) durch Verschlüsselung geschützt.

2.4.6 Konsistenzprüfungen

Übersicht

Security Configuration Tool unterscheidet:

- Lokale Konsistenzprüfungen
- Projektweite Konsistenzprüfungen

Auf welche geprüften Regeln Sie bei der Eingabe achten müssen, finden Sie in den jeweiligen Dialogbeschreibungen unter dem Stichwort "Konsistenzprüfung".

Lokale Konsistenzprüfungen

Eine Konsistenzprüfung heißt lokal, wenn sie direkt innerhalb eines Dialogs durchgeführt werden kann. Bei folgenden Aktionen können Prüfungen ablaufen:

- nach dem Verlassen eines Feldes
- nach dem Verlassen einer Zeile in einer Tabelle
- beim Verlassen des Dialogs mit "OK"

Projektweite Konsistenzprüfungen

Projektweite Konsistenzprüfungen geben Aufschluss über korrekt konfigurierte Baugruppen. Bei folgenden Aktionen erfolgt eine automatische, projektweite Konsistenzprüfung:

- beim Speichern des Projekts
- beim Öffnen des Projekts
- vor dem Laden einer Konfiguration

Hinweis

Projektierdaten können Sie nur laden, wenn das Projekt insgesamt konsistent ist.

So veranlassen Sie eine projektweite Konsistenzprüfung

Führen Sie die Konsistenzprüfung für ein geöffnetes Projekt folgendermaßen durch:

Menübefehl: "Optionen" > "Konsistenzprüfungen...".

Das Prüfergebnis wird in einer Liste ausgegeben, die Sie nach den Meldungstypen "Fehler" oder "Warnungen" filtern können. Wenn das Projekt inkonsistente Daten enthält, wird der Status in der Statuszeile des SCT-Fensters angezeigt. Klicken Sie auf die Statuszeile, um die Prüfliste anzuzeigen.

2.4.7 Symbolische Namen für IP-/MAC-Adressen vergeben

So erreichen Sie diese Funktion

Menübefehl: "Optionen" > "Symbolische Namen ...".

Bedeutung und Vorteil

In einem Security-Projekt können Sie stellvertretend für IP- und MAC-Adressen symbolische Namen in einer Tabelle vergeben.

Die Projektierung der einzelnen Dienste kann dadurch einfacher und sicherer erfolgen.

Bei den folgenden Funktionen und deren Projektierung werden symbolische Namen innerhalb des Projekts berücksichtigt:

- Firewall
- NAT-/NAPT-Router
- Syslog
- DHCP
- NTP

Bildung symbolischer Namen

Symbolischen Namen muss sowohl bei der Definition als auch bei der Verwendung ein Raute-Zeichen (#) vorangestellt werden. Die symbolischen Namen selbst müssen DNS-konform sein.

Gültigkeit und Eindeutigkeit

Die Gültigkeit der in der Tabelle angegebenen symbolischen Namen ist auf die Projektierung innerhalb eines Security-Projekts beschränkt.

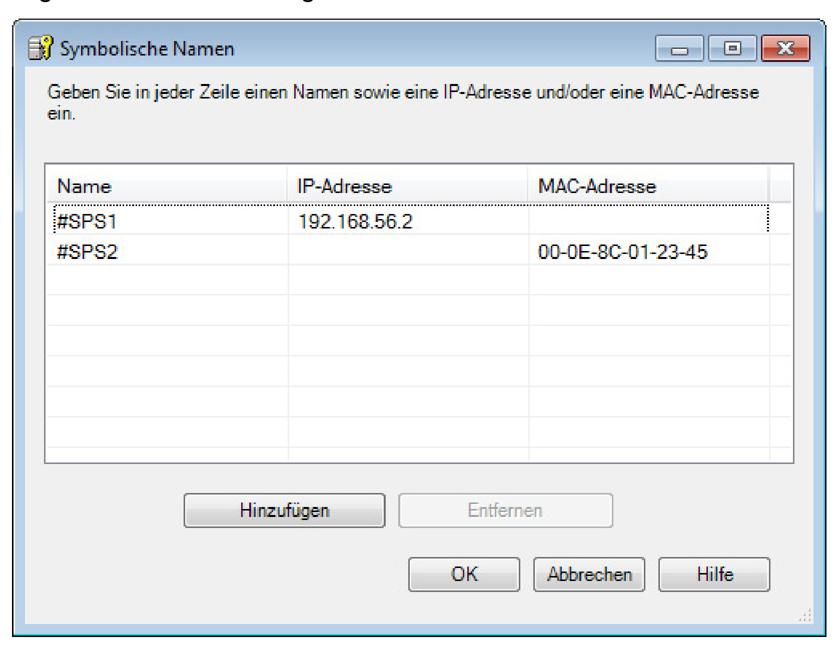
Innerhalb des Projekts muss jeder symbolische Name eindeutig einer einzigen IP-Adresse und/oder MAC-Adresse zugeordnet werden.

Dialog zur Definition symbolischer Namen

Um Inkonsistenzen zwischen einer Zuordnung "IP-Adresse - symbolischer Name" sowie "MAC-Adresse - symbolischer Name" zu vermeiden, werden die symbolischen Namen in einer einzigen Tabelle verwaltet.

Symbolische Namen definieren

1. Betätigen Sie die Schaltfläche "Hinzufügen", um einen neuen symbolischen Namen in der nächsten freien Tabellenzeile hinzuzufügen.
2. Geben Sie ein Raute-Zeichen (#) gefolgt von dem gewünschten symbolischen Namen DNS-konform ein.
3. Ergänzen Sie den Eintrag mit der IP-Adresse und/oder der MAC-Adresse.



Nicht definierte symbolische Namen verwenden

Im Rahmen der Projektierung von Security-Baugruppen können Sie auch symbolische Namen verwenden, die noch nicht definiert sind. Nach dem Eintragen eines noch nicht definierten symbolischen Namens und dem Bestätigen des zugehörigen Dialogs wird der gewählte symbolische Name in die Tabelle der symbolischen Namen aufgenommen. In diesem Dialog können Sie dann die zugehörige IP-Adresse und/oder MAC-Adresse für den symbolischen Namen festlegen.

Falls Sie einen Eintrag in der Tabelle löschen, bleiben die in den Diensten verwendeten symbolischen Namen dort bestehen. Die Konsistenzprüfung erkennt in diesem Falle nicht definierte symbolische Namen. Dies gilt unabhängig davon, ob Sie den symbolischen Namen nachträglich definiert haben oder nicht.

Tipp:

Für die hier beschriebene Tabelle ist die Anwendung der projektweiten Konsistenzprüfung besonders sinnvoll. Sie können anhand der Liste Unstimmigkeiten erkennen und korrigieren.

Starten Sie die Konsistenzprüfung für ein geöffnetes Projekt über den Menübefehl "Optionen" > "Konsistenzprüfungen...".

Konsistenzprüfung - diese Regeln müssen Sie beachten

Berücksichtigen Sie bei Ihrer Eingabe die nachfolgend aufgeführten Regeln:

- Symbolische Namen muss ein Raute-Zeichen (#) vorangestellt werden.
- Die Zuordnung eines symbolischen Namens zu einer IP- oder MAC-Adresse muss eindeutig sein. Der Symbolname und die Adresse dürfen nur einmal vergeben und nicht in einem anderen Listeneintrag verwendet werden.
- Die symbolischen Namen müssen DNS-konform sein.
- Einem symbolischen Namen muss entweder eine IP-Adresse oder eine MAC-Adresse oder beides zugeordnet sein.
- Den IP-Adressen der Security-Baugruppen dürfen keine symbolischen Namen zugewiesen sein.
- Im Projekt für IP- oder MAC-Adressen verwendete symbolische Namen müssen in der Tabelle enthalten sein.

  Inkonsistenzen können dadurch entstehen, dass Einträge in der Tabelle gelöscht und in den Projektierdialogen nicht entsprechend entfernt oder korrigiert werden.

Siehe auch

Konsistenzprüfungen (Seite 63)

DNS-Konformität (Seite 273)

2.5 Benutzer verwalten

2.5.1 Übersicht zur Benutzerverwaltung

Wie ist die Benutzerverwaltung aufgebaut?

Der Zugriff auf die Security-Konfiguration wird durch konfigurierbare Benutzereinstellungen verwaltet. Richten Sie Benutzer mit jeweils einem Passwort zur Authentifizierung ein. Dem Benutzer weisen Sie eine systemdefinierte oder benutzerdefinierte Rolle zu. Den Rollen sind projektierungs- und baugruppenspezifische Rechte zugewiesen. Beachten Sie beim Anlegen die angegebenen Mengengerüste (Seite 20).

Bereits vorhandene Benutzer aus STEP 7 nach SCT migrieren



Bereits in STEP 7 angelegte Benutzer können nach SCT migriert werden. Dabei müssen Sie die Passwörter neu vergeben.

Detailinformationen dazu finden Sie in der Online-Hilfe.



Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen SCT-Dialog.

Eingabereihenfolge beim Anlegen von Benutzern und Rollen

Wählen Sie eine der beiden Eingabereihenfolgen:

- Legen Sie zunächst einen neuen Benutzer an, legen Sie anschließend eine Rolle fest und weisen Sie im letzten Schritt dem Benutzer die Rolle zu.
- Definieren Sie zunächst eine neue Rolle, legen Sie anschließend einen Benutzer an und weisen Sie im letzten Schritt dem Benutzer die Rolle zu.

Hinweis

Verwahren Sie Ihre Benutzer-Passwörter sicher.

Vergessen Sie Ihre Benutzer-Passwörter, haben Sie keinen Zugriff mehr auf das betreffende Projekt bzw. die betreffende Security-Baugruppe.

Sie müssen in diesem Fall ein neues Projekt erstellen und ein "Rücksetzen auf Werkseinstellungen" durchführen. Dabei verlieren Sie aber die Konfiguration.

Hinweis

Werden die Authentifizierungseinstellungen geändert, so müssen die Security-Baugruppen neu geladen werden, damit diese Einstellungen (z. B. neue Benutzer, Passwortänderungen) auf den Security-Baugruppen aktiv werden.

Benutzerauthentifizierung beim Aktivieren benutzerspezifischer IP-Regelsätze S≥V3.0

Die Authentifizierung von Benutzern, die sich auf der Webseite der Security-Baugruppe anmelden, um einen benutzerspezifischen IP-Regelsatz zu aktivieren, kann entweder von der Security-Baugruppe oder von einem RADIUS-Server durchgeführt werden.

Wie Sie für einen Benutzer die Authentifizierungsmethode "RADIUS" festlegen, erfahren Sie in folgendem Kapitel:

- Benutzer anlegen (Seite 69)

Detaillierte Informationen zur Benutzerauthentifizierung durch RADIUS-Server finden Sie in folgendem Kapitel:

- Authentifizierung durch RADIUS-Server (Seite 78)

2.5.2 Benutzer anlegen

So erreichen Sie diese Funktion

Menübefehl SCT: "Optionen" > "Benutzerverwaltung...", Register "Benutzer", Schaltfläche "Hinzufügen...".

Menübefehl STEP 7: "Benutzer" > "Start der Benutzerverwaltung", Schaltfläche "Ausführen". Zusätzlich kann die Benutzerverwaltung aus einzelnen Registern aufgerufen werden.

Parameter	Bedeutung
Benutzername	Frei wählbarer Benutzername.
Authentifizierungsmethode	• **Passwort**: Verwenden Sie diese Authentifizierungsmethode für Benutzer, die das SCT-Projekt bearbeiten und laden sowie die Security-Baugruppe diagnostizieren sollen. Die Authentifizierung des Benutzers wird bei der Aktivierung benutzerspezifischer IP-Regelsätze durch die Security-Baugruppe durchgeführt. • **RADIUS** S≥V4.0 : Die Authentifizierung des Benutzers wird bei der Aktivierung benutzerspezifischer IP-Regelsätze durch einen RADIUS-Server durchgeführt. Das Passwort des Benutzers wird bei dieser Authentifizierungsmethode nicht in SCT projektiert, sondern Sie müssen dieses auf dem RADIUS-Server hinterlegen. Verwenden Sie diese Authentifizierungsmethode ausschließlich für Benutzer, die sich lediglich auf der Webseite einer Security-Baugruppe anmelden sollen. Ein Benutzer mit der Authentifizierungsmethode "RADIUS" kann sich nicht an SCT-Projekten anmelden.
Passwort (nur bei der Authentifizierungsmethode "Passwort")	Eingabe des Passworts für den Benutzer. Bei der Eingabe wird die Passwortstärke überprüft. Nähere Informationen zur Passwortstärke finden Sie in folgendem Kapitel: Regeln für Benutzernamen, Rollen und Passwörter (Seite 21)
Passwort wiederholen (nur bei der Authentifizierungsmethode "Passwort")	Wiederholung des eingegebenen Passworts.
Kommentar	Zusätzliche Kommentareingabe.
Maximale Sitzungsdauer S≥V3.0	Eingabe der Zeitdauer, nach welcher ein Benutzer, der auf der Webseite für benutzerspezifische IP-Regelsätze von SCALANCE S Baugruppen angemeldet ist, automatisch abgemeldet wird. Die hier angegebene Zeitdauer beginnt nach der Anmeldung sowie nach dem Erneuern der Sitzung auf der Webseite der Security-Baugruppe. • Standardeinstellung: 30 Minuten • Mindestwert: 5 Minuten • Maximalwert: 480 Minuten
Zugewiesene Rolle	Je nach getroffener Zuordnung.

Tabelle 2- 1 Schaltflächen im Register "Benutzer"

Bezeichnung	Bedeutung / Auswirkung
Bearbeiten...	Markieren Sie einen Eintrag und klicken Sie auf die Schaltfläche. Im aufgeblendeten Dialog ändern Sie die oben aufgeführten Einstellungen.
Hinzufügen...	Fügen Sie über die Schaltfläche einen neuen Benutzer hinzu.
Löschen	Löschen Sie über die Schaltfläche den ausgewählten Eintrag. **Hinweis** Im Projekt muss immer mindestens ein Benutzer mit der Rolle "Administrator" vorhanden sein. Der Administrator, der bei Projekterstellung automatisch angelegt wird, kann nur gelöscht werden, solange mindestens ein weiterer Benutzer mit vollständigen Projektierungsrechten existiert.

2.5.3 Rollen anlegen

Welche Rollen gibt es?

Sie können einem Benutzer eine systemdefinierte oder benutzerdefinierte Rolle zuweisen. Die Baugruppenrechte einer benutzerdefinierten Rolle legen Sie pro Security-Baugruppe fest.

Systemdefinierte Rollen

Vordefiniert sind die folgenden systemdefinierten Rollen. Den Rollen sind bestimmte Rechte zugewiesen, die auf allen Baugruppen gleich sind und die der Administrator nicht ändern oder löschen kann.

Rechte verwalten (Seite 72)

- administrator

  Standardmäßige Rolle beim Anlegen eines neuen SCT-Projekts.

  Uneingeschränkte Zugriffsrechte auf alle Konfigurationsdaten.
- standard

  Rolle mit eingeschränkten Zugriffsrechten.
- diagnostics

  Standardmäßige Rolle beim Anlegen eines neuen Benutzers.

  Nur lesender Zugriff.
- remote access

  Keine Rechte außer Anmeldung an der Webseite für benutzerspezifische IP-Regelsätze.

- radius

  Rolle, die zur Aktivierung benutzerspezifischer IP-Regelsätze mit Authentifizierung über RADIUS-Server verwendet werden kann.

  Nur lesender Zugriff.

- administrator (radius)

  Rolle, die zur Aktivierung benutzerspezifischer IP-Regelsätze mit Authentifizierung über RADIUS-Server verwendet werden kann.

  Zugriffsrechte auf alle Konfigurationsdaten außer auf SNMP-MIBs.

Hinweis

Weitere Informationen zu benutzerspezifischen IP-Regelsätzen finden Sie in folgendem Kapitel:

Benutzerspezifische IP-Regelsätze (Seite 143)

Hinweis

Weitere Informationen zur Authentifizierung über RADIUS-Server finden Sie in folgendem Kapitel:

Authentifizierung durch RADIUS-Server (Seite 78)

Benutzerdefinierte Rolle

Zusätzlich zu den systemdefinierten Rollen können Sie benutzerdefinierte Rollen anlegen. Für eine benutzerdefinierte Rolle wählen Sie die Projektierungs- bzw. Baugruppenrechte und legen für jede im Projekt verwendete Security-Baugruppe die entsprechenden Rechte fest. Die benutzerdefinierten Rollen weisen Sie dem entsprechenden Benutzer manuell zu.

So erreichen Sie diese Funktion

Menübefehl SCT: "Optionen" > "Benutzerverwaltung...", Register "Rollen".

Menübefehl STEP 7: "Benutzer" > "Start der Benutzerverwaltung", Schaltfläche "Ausführen". Zusätzlich kann die Benutzerverwaltung aus einzelnen Registern aufgerufen werden.

Tabelle 2- 2 Angaben im Register "Rollen"

Parameter	Bedeutung
Rollenname	Frei wählbarer Rollenname.
Kommentar	Zusätzliche Kommentareingabe.
Maximale Sitzungsdauer S≥V3.0	Eingabe der Zeitdauer, nach welcher ein Benutzer mit der zugeordneten Rolle von der Webseite für benutzerspezifische IP-Regelsätze von SCALANCE S Baugruppen automatisch abgemeldet wird. Die hier angegebene Zeitdauer beginnt nach der Anmeldung sowie nach dem Erneuern der Sitzung auf der Webseite der Security-Baugruppe. • Standardeinstellung: 30 Minuten • Mindestwert: 5 Minuten • Maximalwert: 480 Minuten

Tabelle 2- 3 Schaltflächen im Register "Rollen"

Bezeichnung	Bedeutung / Auswirkung
Eigenschaften... / Bearbeiten...	Markieren Sie in der Liste eine benutzerdefinierte Rolle und klicken Sie auf die Schaltfläche. Im aufgeblendeten Dialog ändern Sie die Eigenschaften der Rolle, wie den Rollennamen, die der Rolle zugewiesenen Rechte sowie die maximale Sitzungsdauer. Systemdefinierte Rollen können nicht bearbeitet werden.
Hinzufügen...	Fügen Sie über die Schaltfläche eine neue benutzerdefinierte Rolle hinzu. Im aufgeblendeten Dialog geben Sie den Rollennamen ein und weisen der Rolle aus der Rechteliste die entsprechenden Rechte zu. Angezeigt werden die Rechte der in der Rechtevorlage ausgewählten systemdefinierten Rolle (Standardvorlage: "diagnostics").
Löschen	Löschen Sie über die Schaltfläche den ausgewählten Eintrag. **Hinweis** • Eine bereits erzeugte benutzerdefinierte Rolle kann nur gelöscht werden, wenn sie keinem Benutzer zugewiesen ist. Weisen Sie dem Benutzer gegebenenfalls eine andere Rolle zu. • Systemdefinierte Rollen können nicht gelöscht werden.

2.5.4 Rechte verwalten

So erreichen Sie diese Funktion

Menübefehl SCT: "Optionen" > "Benutzerverwaltung...", Register "Rollen", Schaltfläche "Eigenschaften..." bzw. "Hinzufügen…".

Menübefehl STEP 7: "Benutzer" > "Start der Benutzerverwaltung", Schaltfläche "Ausführen". Zusätzlich kann die Benutzerverwaltung aus einzelnen Registern aufgerufen werden.

Benutzerdefinierte Rolle erstellen und zuweisen

1. Geben Sie einen Rollennamen ein.
2. Wählen Sie aus der Rechtevorlage eine systemdefinierte Rolle aus (Standardvorlage: "diagnostics"). Benutzerdefinierte Rollen werden in der Auswahl nicht angezeigt.

   Ergebnis: Entsprechend der ausgewählten Rolle werden für jede im Projekt verwendete Security-Baugruppe in der Rechteliste die dazugehörenden Rechte angezeigt. Die Rechte der nicht im Projekt verwendeten Security-Baugruppen sind ausgegraut.
3. Aktivieren bzw. deaktivieren Sie für jede Security-Baugruppe die Rechte, die der benutzerdefinierten Rolle zugewiesen werden sollen.
4. Geben Sie ggf. einen Kommentar sowie eine maximale Sitzungsdauer für die zu erstellende Rolle ein.
5. Klicken Sie auf die Schaltfläche "Übernehmen" um die Auswahl zu speichern bzw. "OK" um zu speichern und das Fenster zu schließen.
6. Weisen Sie die Rolle einem Benutzer zu.

Rollenrecht einer Security-Baugruppe kopieren

Wählen Sie im Kontextmenü einer Security-Baugruppe aus der Objektliste den Befehl "Rechte kopieren..." und weisen Sie diese über den Befehl "Rechte einfügen..." einer anderen Security-Baugruppe zu.

Projektierungsrechte

Je nach Rollentyp stehen Ihnen pro Security-Projekt die folgenden Projektierungsrechte zur Auswahl:

Tabelle 2- 4 Projektierungsrechte für Zugriffe auf das Security-Projekt

Projektierungsrecht	administrator	standard	diagnostics
Security diagnostizieren	x	x	x
Security konfigurieren	x	x	-
Benutzer und Rollen verwalten	x	-	-

x Recht ist aktiviert

- Recht ist deaktiviert

Baugruppenrechte

In der Spalte "Dienst" wird das System angezeigt, auf welches das jeweilige Recht Auswirkungen hat.

Je nach Rollentyp stehen Ihnen pro Security-Projekt die folgenden Baugruppenrechte zur Auswahl:

Tabelle 2- 5 Baugruppenrechte CP x43-1 Adv.

Recht innerhalb des Dienstes	administrator	standard	diagnostics	Dienst
Web: CP-Dateisystem formatieren *	x	-	-	Dateisystem
FTP: Dateien vom CP-Dateisystem lesen	x	x	x	
FTP: Dateien auf das CP-Dateisystem schreiben	x	x	-	
FTP: Dateien (DBs) von der S7-CPU lesen **	x	x	x	SPS
FTP: Dateien (DBs) in die S7-CPU schreiben ***	x	x	-	
Applet: Variablen über projektierte Symbole lesen *	x	x	x	
Applet: Variablen über projektierte Symbole schreiben *				
Applet: Variablen über absolute Adressen lesen *	x	x	x	
Applet: Variablen über absolute Adressen schreiben *	x	x	-	
Applet: Status der Baugruppen im Rack lesen *	x	x	x	
Applet: Bestellnummer der Baugruppen im Rack lesen *	x	x	x	
SNMP: MIB-II lesen	x	x	x	SNMP
SNMP: MIB-II schreiben	x	x	-	
SNMP: Automation-MIB lesen	x	x	x	
SNMP: LLDP-MIB lesen	x	x	x	
SNMP: SNMPv2-MIB lesen	x	x	x	
SNMP: MRP-MIB lesen	x	x	x	
SNMP: MRP-MIB schreiben	x	x	-	
SCT: Diagnose der Security-Baugruppe durchführen ****	x	x	x	Sicherheit
Web: IP Access Control-Liste erweitern *	x	-	-	
Web: Auf Web-Diagnose und CP-Dateisystem zugreifen	x	x	x	Web
Web: Testmail versenden *	x	x	x	
Web: Firmware aktualisieren *	x	x	-	Wartung
Web: Nachladen von Diagnosetexten *	x	x	-	

x Recht ist aktiviert

- Recht ist deaktiviert

* Um die Funktion anzuwenden, muss das Baugruppenrecht "Web: Auf Web-Diagnose und CP-Dateisystem zugreifen" ebenfalls aktiviert sein.

** Um die Funktion anzuwenden, muss das Baugruppenrecht "FTP: Dateien vom CP-Dateisystem lesen" ebenfalls aktiviert sein.

*** Um die Funktion anzuwenden, muss das Baugruppenrecht "FTP: Dateien auf das CP-Dateisystem schreiben" ebenfalls aktiviert sein.

**** Um die Funktion anzuwenden, muss das Projektierungsrecht "Security diagnostizieren" ebenfalls aktiviert sein.

Tabelle 2- 6 Baugruppenrechte CP 1628

Recht innerhalb des Dienstes	administrator	standard	diagnostics	Dienst
SNMP: MIB-II lesen	x	x	x	SNMP
SNMP: MIB-II schreiben	x	x	-	
SNMP: Automation-MIB lesen	x	x	x	
SNMP: SNMPv2-MIB lesen	x	x	x	
SCT: Diagnose der Security-Baugruppe durchführen	x	x	x	Sicherheit

x Recht ist aktiviert

\- Recht ist deaktiviert

Tabelle 2- 7 Baugruppenrechte SCALANCE S ≥ V3.0

Recht innerhalb des Dienstes	administrator	standard	diagnostics	Dienst
SNMP: MIB-II lesen	x	x	x	SNMP
SNMP: MIB-II schreiben	x	x	-	
SNMP: Automation-MIB lesen	x	x	x	
SNMP: SNMPv2-MIB lesen	x	x	x	
SNMP: MRP-MIB lesen S627-2M	x	x	x	
SNMP: MRP-MIB schreiben S627-2M	x	x	-	
SCT: Diagnose der Security-Baugruppe durchführen	x	x	x	Sicherheit
Laden der Konfigurationsdateien	x	x	-	
Web: Firmware aktualisieren	x	x	-	Wartung

x Recht ist aktiviert

\- Recht ist deaktiviert

Tabelle 2- 8 Baugruppenrechte SCALANCE S < V3.0

Recht innerhalb des Dienstes	administrator	standard	diagnostics	Dienst
Laden der Konfigurationsdateien	x	x	-	Sicherheit
SCT: Diagnose der Security-Baugruppe durchführen	x	x	x	

x Recht ist aktiviert

\- Recht ist deaktiviert

Einstellen von Baugruppenrechten vor und nach dem Anlegen von Security-Baugruppen

Innerhalb einer benutzerdefinierten Rolle werden die Baugruppenrechte für jede Security-Baugruppe separat definiert. Wurde eine Security-Baugruppe, für die die Baugruppenrechte innerhalb einer Rolle definiert werden sollen, vor dem Hinzufügen der Rolle angelegt, dann werden die Baugruppenrechte für diese Security-Baugruppe gemäß der ausgewählten Rechtevorlage automatisch eingestellt und können bei Bedarf angepasst werden. Wurde eine Security-Baugruppe nach dem Anlegen einer Rolle hinzugefügt, dann werden von SCT keine Rechte gesetzt. In diesem Fall müssen Sie alle Baugruppenrechte für die Security-Baugruppe selbst einstellen.

Bereits bestehende Baugruppenrechte können Sie auch durch Kopieren auf eine andere Security-Baugruppe übernehmen und dort ggf. anpassen. Wählen Sie hierzu im Kontextmenü einer Security-Baugruppe in den Baugruppenrechten den Menübefehl "Rechte kopieren..." bzw. "Rechte einfügen...".

2.5.5 Passwort-Richtlinien projektieren

Bedeutung

Mit Hilfe der Passwort-Richtlinien lassen sich Vorgaben definieren, die bei der Vergabe von Passwörtern an neue Benutzer beachtet werden müssen.

So erreichen Sie diese Funktion

Wählen Sie den Menübefehl "Optionen" > "Benutzerverwaltung...", Register "Passwort-Richtlinien". Nach dem Aktivieren eines Kontrollkästchens ist die zugehörige Richtlinie aktiv und kann ggf. über das jeweilige Eingabefeld angepasst werden.

Parameter	Bedeutung
Minimale Passwortlänge	Anzahl an Zeichen, die Passwörter mindestens enthalten müssen. Das zugehörige Kontrollkästchen ist standardmäßig aktiviert und kann nicht deaktiviert werden. • Mindestwert: 8 Zeichen • Maximalwert: 32 Zeichen
Minimale Anzahl an Zahlen	Anzahl an Zahlen, die Passwörter mindestens enthalten müssen. • Mindestwert: 1 Zahl • Maximalwert: 32 Zahlen
Minimale Anzahl an Sonderzeichen	Anzahl an Sonderzeichen, die Passwörter mindestens enthalten müssen. Ein Sonderzeichen ist jedes Zeichen, welches weder ein Buchstabe noch eine Zahl ist. • Mindestwert: 1 Sonderzeichen • Maximalwert: 32 Sonderzeichen

Parameter	Bedeutung
Anzahl der zur Wiederverwendung gesperrten Passwörter	Anzahl der zuletzt verwendeten Passwörter, die bei einer Passwortänderung als neues Passwort nicht zur Verfügung stehen. • Mindestwert: 1 Passwort • Maximalwert: 10 Passwörter
Mindestens ein Groß- und Kleinbuchstabe	Wenn Sie dieses Kontrollkästchen aktivieren, müssen Passwörter mindestens einen Großbuchstaben und einen Kleinbuchstaben enthalten.

2.5.6 Authentifizierung durch RADIUS-Server

2.5.6.1 Übersicht

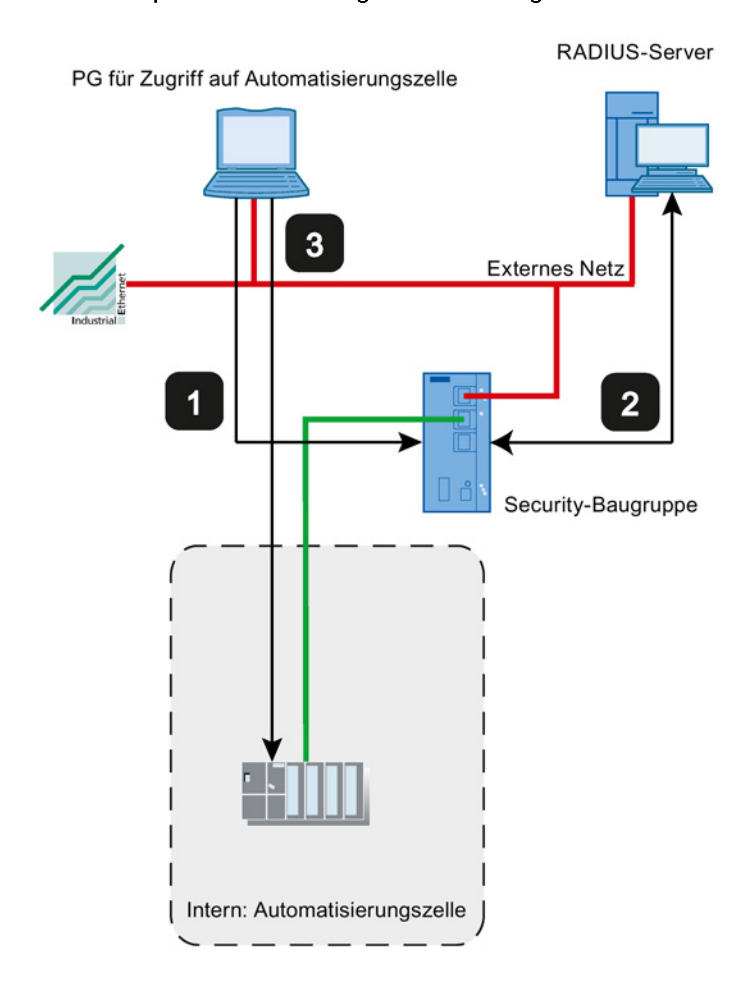


Bedeutung

RADIUS (Remote Authentication Dial-In User Service) ist ein Protokoll zur Authentifizierung von Benutzern durch Server, auf denen Benutzerdaten zentral abgelegt werden können. Durch den Einsatz von RADIUS-Servern kann der Schutz von Benutzernamen, zugeordneten Rollen und Passwörtern erhöht werden.

Einsatzszenario von RADIUS-Servern

Die Authentifizierung durch RADIUS-Server kann im Rahmen der Aktivierung benutzerspezifischer IP-Regelsätze durchgeführt werden.



1 Eingabe der Benutzerdaten auf der Webseite der Security-Baugruppe
2 Authentifizierung durch RADIUS-Server und Aktivierung des benutzerspezifischen IP-Regelsatzes
3 Zugriff auf Automatisierungszelle

Der oben dargestellte Netzaufbau ist exemplarisch. Der RADIUS-Server kann sich auch im internen Netz oder im DMZ-Netz der Security-Baugruppe befinden.

Für die im Folgenden beschriebenen Projektierungsmöglichkeiten wird jeweils vorausgesetzt, dass ein RADIUS-Server in SCT projektiert und der jeweiligen Security-Baugruppe zugeordnet wurde. Zudem muss ein Benutzer bzw. eine Rolle mit der Authentifizierungsmethode "RADIUS" projektiert sein. Informationen hierzu finden Sie in folgenden Kapiteln:

- RADIUS-Server definieren (Seite 80)
- RADIUS-Server einer Security-Baugruppe zuweisen (Seite 82)
- Benutzer anlegen (Seite 69)
- Rollen anlegen (Seite 70)

Generelle Informationen zu benutzerspezifischen IP-Regelsätzen finden Sie in folgendem Kapitel:

- Benutzerspezifische IP-Regelsätze (Seite 143)

Projektierungsmöglichkeiten

Für die Authentifizierung des Benutzers durch einen RADIUS-Server stehen zwei Projektierungsmöglichkeiten zur Verfügung:

- Der Benutzer ist mit seiner Rolle auf der Security-Baugruppe bekannt, lediglich die Passwortverwaltung für den Benutzer erfolgt über den RADIUS-Server. Auf dem RADIUS-Server ist der Benutzer mit zugehörigem Passwort konfiguriert.
  - Es wird ein Benutzer mit der Authentifizierungsmethode "RADIUS" projektiert.
  - Dem benutzerspezifischen IP-Regelsatz wird der Benutzer zugewiesen.

  Ergebnis:
  - Bei der Anmeldung eines Benutzers an der Webseite der Security-Baugruppe wird die Authentifizierungsanfrage an den RADIUS-Server weitergeleitet.
  - Der RADIUS-Server führt eine Passwortprüfung durch und meldet das Ergebnis an die Security-Baugruppe zurück.
  - Ist die Passwortprüfung bestanden, wird der benutzerspezifische IP-Regelsatz aktiviert.

- Die Rolle ist auf der Security-Baugruppe bekannt, die Benutzerverwaltung erfolgt über den RADIUS-Server. Auf dem RADIUS-Server ist der Benutzer mit zugehörigem Passwort konfiguriert.
  - Dem benutzerspezifischen IP-Regelsatz wird eine benutzerdefinierte Rolle oder eine systemdefinierte Rolle zugewiesen.
  - Im Register "RADIUS" der Security-Baugruppe wird das Kontrollkästchen "RADIUS-Authentifizierung nicht projektierter Benutzer erlauben" sowie das Kontrollkästchen "Filter-ID wird für die Authentifizierung benötigt" aktiviert.

  Ergebnis:
  - Bei der Anmeldung eines Benutzers an der Webseite der Security-Baugruppe wird die Authentifizierungs- und Autorisierungsanfrage an den RADIUS-Server weitergeleitet.
  - Der RADIUS-Server führt eine Passwortprüfung durch und meldet das Ergebnis an die Security-Baugruppe zurück.
  - Fall a: Wenn zusätzlich der Rollenname auf dem RADIUS-Server projektiert ist:

    Der RADIUS-Server gibt den dem Benutzer zugeordneten Rollennamen an die Security-Baugruppe zurück.
  - Fall b: Wenn der Rollenname auf dem RADIUS-Server nicht projektiert ist:

    Die Security-Baugruppe vergibt dem Benutzer die systemdefinierte Rolle "radius".
  - Ist die Passwortprüfung bestanden, wird der benutzerspezifische IP-Regelsatz aktiviert.

Vereinbarungen für RADIUS-Server

- Die RADIUS-Server können sich in jedem mit der Security-Baugruppe verbundenen Netzwerk befinden.
- Es können maximal zwei RADIUS-Server pro Security-Baugruppe projektiert werden. Im Betrieb ist dann jeweils nur einer der RADIUS-Server aktiv.
- Bei der Definition eines RADIUS-Servers kann anstelle einer IP-Adresse auch ein FQDN verwendet werden.

2.5.6.2 RADIUS-Server definieren



Bedeutung

Bevor die Authentifizierung durch einen RADIUS-Server erfolgen kann, müssen Sie diesen zunächst im SCT-Projekt hinterlegen. Im Anschluss müssen Sie den definierten RADIUS-Server der Security-Baugruppe zuweisen, für welche der RADIUS-Server die Benutzerauthentifizierung übernehmen soll.

Vorgehensweise

1. Wählen Sie den Menübefehl "Optionen" > "Konfiguration der RADIUS-Server...".
2. Klicken Sie auf die Schaltfläche "Hinzufügen...".
3. Geben Sie die erforderlichen Parameter gemäß der folgenden Tabelle an.

Parameter	Bedeutung
Name	Frei wählbarer Name für den RADIUS-Server.
IP-Adresse / FQDN	IP-Adresse oder FQDN des RADIUS-Servers.
Port	UDP-Port, unter welchem der RADIUS-Server erreichbar ist. Standardmäßig werden Authentifizierungsdaten an Port 1812 empfangen.
Shared-Secret	Eingabe des Passworts, das bei der Übertragung der Anmeldedaten zwischen RADIUS-Server und Security-Baugruppen zur Verschlüsselung verwendet wird. Erlaubt sind folgende Zeichen des Zeichensatzes ANSI X 3.4-1986: 0123456789 A...Z a...z !#$%&()"*'+`,-./:;<=>?@ [\]_{|}~^ Länge des Shared-Secrets: 1 ... 31 Zeichen
Shared-Secret wiederholen	Bestätigung des Passworts.
Authentifizierungsmethode	Anzeige des Verfahrens, das zur Überprüfung der Benutzerdaten verwendet wird. Es wird ausschließlich das Verfahren "PAP" (Password Authentication Protocol) unterstützt.
Kommentar	Frei wählbare, optionale Kommentareingabe.

Ergebnis

Sie haben einen RADIUS-Server definiert und können diesen nun den gewünschten Security-Baugruppen zuweisen.

2.5.6.3 RADIUS-Server einer Security-Baugruppe zuweisen



Voraussetzung

Sie haben einen RADIUS-Server definiert.

Vorgehensweise

1. Selektieren Sie die Security-Baugruppe, der Sie einen RADIUS-Server zuweisen möchten.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...".
3. Wählen Sie das Register "RADIUS".
4. Aktivieren Sie das Kontrollkästchen "RADIUS-Authentifizierung aktivieren".

Hinweis

Änderung der Methode zur Authentifizierung mit Webserver auf Security-Baugruppe

Wenn die RADIUS-Authentifizierung auf der Security-Baugruppe aktiviert wird, wird die Methode zur Authentifizierung mit dem Webserver von "Digest Access Authentication" auf "Basic Access Authentication" umgestellt.

---

5. Geben Sie in das Eingabefeld "RADIUS-Timeout" die Zeit in Sekunden ein, die die Security-Baugruppe maximal auf eine Antwort des RADIUS-Servers warten soll.
6. Geben Sie in das Eingabefeld "RADIUS-Wiederholungen" die Anzahl der Verbindungsversuche mit dem RADIUS-Server ein.
7. Aktivieren Sie das Kontrollkästchen "RADIUS-Authentifizierung nicht projektierter Benutzer erlauben", wenn dem zu aktivierenden, benutzerspezifischen IP-Regelsatz anstelle eines Benutzers eine Rolle zugewiesen wurde.
8. Aktivieren Sie das Kontrollkästchen "Filter-ID wird für die Authentifizierung benötigt", wenn es sich bei der zugewiesenen Rolle um eine benutzerdefinierte Rolle handelt.
9. Klicken Sie auf die Schaltfläche "Hinzufügen".

   Ergebnis: Der RADIUS-Server, der als erstes projektiert wurde, wird der Security-Baugruppe zugewiesen.
10. Wählen Sie ggf. aus der Klappliste "Name" den RADIUS-Server, den Sie der Security-Baugruppe zuweisen möchten.

Generelle Informationen zur Authentifizierung durch RADIUS-Server finden Sie in folgendem Kapitel:
Authentifizierung durch RADIUS-Server (Seite 78)

Siehe auch

Benutzer anlegen (Seite 69)

2.6 Zertifikate verwalten

2.6.1 Übersicht

Wie verwalten Sie Zertifikate?

Im Zertifikatsmanager erhalten Sie eine Übersicht aller im Projekt verwendeten Zertifikate / CA-Zertifikate mit Angaben zu Antragssteller, Aussteller, Gültigkeit, Verwendung in SCT und Vorhandensein eines privaten Schlüssels.

Das CA-Zertifikat ist ein durch eine Zertifizierungsstelle, die so genannte "Certificate Authority", ausgestelltes Zertifikat, von denen die Gerätezertifikate abgeleitet werden. Zu den Gerätezertifikaten gehören die SSL-Zertifikate, die zur Authentifizierung bei der Online-Kommunikation zwischen einer Security-Baugruppe und einem weiteren Netzwerkteilnehmer benötigt werden. Weitere Gerätezertifikate sind die VPN-Gruppen-Zertifikate von Security-Baugruppen, die sich in VPN-Gruppen befinden. Zertifizierungsstellen können sein:

- SCT selbst. Sind "Antragsteller" und "Aussteller" gleich, dann handelt es sich um ein selbst-signiertes, also durch SCT ausgestelltes Zertifikat.
- Eine übergeordnete Zertifizierungsstelle. Diese projektexternen Fremdzertifikate werden importiert und im Zertifikatsspeicher von SCT abgelegt.

Zertifikate, die von einer der beiden Zertifizierungsstellen angelegt werden, haben immer einen privaten Schlüssel, damit die Gerätezertifikate abgeleitet werden können.

Zusätzlich stehen Ihnen im Zertifikatsmanager die folgenden Funktionen zur Auswahl:

- Importieren von neuen Zertifikaten und Zertifizierungsstellen.
- Importieren von FTPS-Zertifikaten, wenn der CP als FTP-Client verwendet wird. 

- Exportieren der im Projekt verwendeten Zertifikate und Zertifizierungsstellen.
- Erneuern von abgelaufenen Zertifikaten und Zertifizierungsstellen.
- Ersetzen bestehender Zertifizierungsstellen.

Hinweis

Laden des Projekts

Nach dem Ersetzen oder Erneuern von Zertifikaten muss das Projekt auf die entsprechende Security-Baugruppe geladen werden.

Nach dem Ersetzen oder Erneuern von CA-Zertifikaten muss das Projekt auf alle Security-Baugruppen geladen werden.

Hinweis

Aktuelles Datum und aktuelle Uhrzeit auf den Security-Baugruppen

Achten Sie bei der Verwendung von gesicherter Kommunikation (z. B. HTTPS, VPN...) darauf, dass die betroffenen Security-Baugruppen über die aktuelle Uhrzeit und das aktuelle Datum verfügen. Die verwendeten Zertifikate werden sonst als nicht gültig ausgewertet und die gesicherte Kommunikation funktioniert nicht.

So erreichen Sie diese Funktion

Menübefehl SCT: "Optionen" > "Zertifikatsmanager…".

In den einzelnen Registern stehen Ihnen die folgenden Schaltflächen zur Verfügung:

Schaltfläche	Beschreibung
Importieren... / Exportieren...	Import / Export von Gerätezertifikaten bzw. CA-Zertifikaten, die nicht in SCT angelegt wurden. Die Zertifikate werden auf die Security-Baugruppe übertragen. Folgende Formate sind erlaubt: *.pem (nur Zertifikat) *.crt (nur Zertifikat) *.p12 (Zertifikat mit dazugehörigem privaten Schlüssel) **Hinweis** • Benutzer mit der systemdefinierten Rolle "diagnostics" dürfen keinen Export durchführen.
Anzeigen...	Öffnet den Zertifikatsdialog von Windows, in dem Sie eine Übersicht aller Zertifikatsdaten angezeigt bekommen.

Register "Zertifizierungsstellen"

Die hier angezeigten Zertifikate werden durch eine Zertifizierungsstelle angelegt.

- Zertifizierungsstelle eines Projekts: Beim Erstellen eines neuen SCT-Projekts wird für das Projekt ein CA-Zertifikat erzeugt. Von diesem Zertifikat werden die SSL-Zertifikate für die einzelnen Security-Baugruppen abgeleitet.
- Zertifizierungsstelle einer VPN-Gruppe: Beim Erstellen einer neuen VPN-Gruppe wird für die VPN-Gruppe ein CA-Zertifikat erzeugt. Von diesem Zertifikat werden die VPN-Gruppen-Zertifikate von Security-Baugruppen abgeleitet, die sich in der zugehörigen VPN-Gruppe befinden.

Register "Gerätezertifikate"

Anzeige der gerätespezifischen Zertifikate, die von SCT für eine Security-Baugruppe erzeugt werden. Dazu gehören:

- SSL-Zertifikat einer Security-Baugruppe: Für jede angelegte Security-Baugruppe wird ein SSL-Zertifikat erzeugt, das aus dem CA-Zertifikat des Projekts abgeleitet ist. SSL-Zertifikate werden zur Authentifizierung bei der Kommunikation zwischen PG/PC und

Security-Baugruppe, beim Laden der Konfiguration (nicht für CPs) sowie beim Logging herangezogen.

- VPN-Gruppen-Zertifikat einer Security-Baugruppe: Zusätzlich wird für jede Security-Baugruppe pro VPN-Gruppe, in der sie sich befindet, ein VPN-Gruppen-Zertifikat erzeugt.

Register "Vertrauenswürdige Zertifikate und Stammzertifizierungsstellen"

Anzeige der in SCT importierten Fremdzertifikate. Importiert werden können z. B. Server-Zertifikate von externen FTP-Servern oder Projektzertifikate von anderen SCT-Projekten.



Das importierte Fremdzertifikat wird auf alle im SCT-Projekt verwalteten CPs übertragen. Mit diesem Zertifikat kann sich die Security-Baugruppe dann z. B. beim Zugriff auf einen FTPS-Server ausweisen. Die SCT-Projektierung selbst verwendet das importierte Zertifikat nicht.



Anzeige der Zertifizierungsstellen, die für die Verifizierung externer Dienste wie Anbieter von dyn. DNS durch Security-Baugruppen notwendig sind.

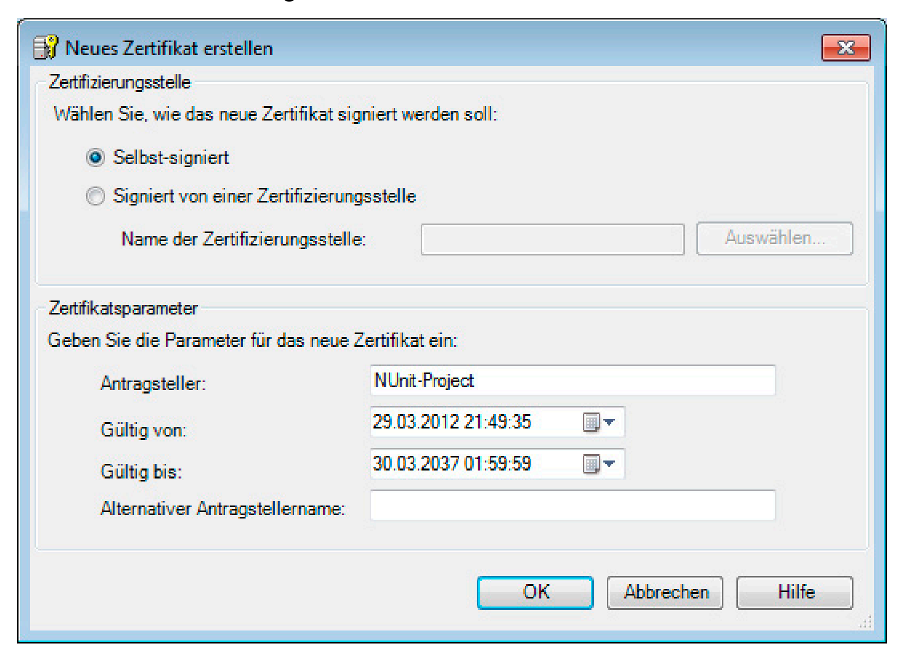
2.6.2 Zertifikate erneuern

Bedeutung

In diesem Dialog erneuern Sie CA-Zertifikate und Gerätezertifikate. Sie können bei Bedarf, z. B. bei kompromittierten Zertifikaten, ein Zertifikat importieren oder ein neues Zertifikat vom Security Configuration Tool erzeugen lassen.

So erreichen Sie diese Funktion

1. Klicken Sie mit der rechten Maustaste auf einen Listeneintrag im Zertifikatsmanager.
2. Wählen Sie den Eintrag "Zertifikat erneuern ...".



3. Wählen Sie aus, ob das neue Zertifikat selbst-signiert oder durch eine Zertifizierungsstelle signiert werden soll.
4. Wenn das Zertifikat durch eine Zertifizierungsstelle signiert werden soll, wählen Sie über die Schaltfläche "Auswählen..." die zu verwendende Zertifizierungsstelle aus. Zur Auswahl stehen dabei nur Zertifizierungsstellen, die im Zertifikatsspeicher des aktuellen SCT-Projekts abgelegt sind.
5. Wählen Sie einen Zeitraum aus, in dem das Zertifikat gültig ist. Standardmäßig wird in die Felder "Gültig von:" und "Gültig bis:" der Wert des aktuellen Zertifikats eingetragen.
6. Geben Sie je nach Zertifikat die folgenden Werte ein:

Zu erneuerndes Zertifikat	Parameter	
	Antragssteller	Alternativer Antragstellername
CA-Zertifikat des Projekts	Name des CA-Zertifikats	-
CA-Zertifikat von VPN-Gruppe	Name des CA-Zertifikats	-
SSL-Zertifikat für S7-CP	Name der Security-Baugruppe	IP-Adressen der Gigabit- und PROFINET-Schnittstelle, durch ein Komma getrennt.
SSL-Zertifikat für PC-CP	Name der Security-Baugruppe	IP-Adresse der Security-Baugruppe.

Zu erneuerndes Zertifikat	Parameter	
	Antragssteller	Alternativer Antragstellername
SSL-Zertifikat für SCALANCE S, SCALANCE M und SOFTNET Security Client	Name der Security-Baugruppe	-
VPN-Gruppen-Zertifikat einer Security-Baugruppe	Name des VPN-Gruppen-Zertifikats	Von der CA abgeleitet.

2.6.3 Zertifikate ersetzen

Bedeutung

In dem Dialog ersetzen Sie das bestehende CA-Zertifikat des Projekts oder das CA-Zertifikat einer VPN-Gruppe durch ein neues.

So erreichen Sie diese Funktion

1. Klicken Sie mit der rechten Maustaste auf einen Listeneintrag im Register "Zertifizierungsstellen".
2. Wählen Sie den Eintrag "Zertifikat ersetzen...".
3. Der Dialog "Zertifizierungsstelle austauschen" wird geöffnet.

Alle im Feld "Betroffene Zertifikate" aufgelisteten Zertifikate werden neu abgeleitet. Somit kann das CA-Zertifikat einer bereits projektierten VPN-Gruppe innerhalb des SCT-Projekts durch das CA-Zertifikat einer VPN-Gruppe aus einem anderen SCT-Projekt ersetzt werden. Die VPN-Gruppen-Zertifikate für die Teilnehmer der VPN-Gruppe werden also in beiden Projekten von dem gleichen CA-Zertifikat abgeleitet.

Falls beim Schließen des Zertifikatmanagers ein Hinweisdialog erscheint, laden Sie die geänderte Konfiguration erneut auf die Security-Baugruppe.

Welches Format darf das Zertifikat haben?

Von dem importierten CA-Zertifikat werden weitere Zertifikate in SCT abgeleitet. Deshalb können Sie nur Zertifikate mit privatem Schlüssel auswählen:

- *.p12

3 Baugruppen anlegen und Netzparameter einstellen

Das vorliegende Kapitel macht Sie damit vertraut, wie Baugruppen angelegt werden und welche Einstellungen für die einzelnen Baugruppen in einem Projekt möglich sind.

Weitere Informationen



Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen SCT-Dialog.

Hinweis

Leistungsmerkmale und Gerätetypen

Beachten Sie bei dem von Ihnen verwendeten Gerätetyp, welche Funktionen jeweils unterstützt werden.

Siehe auch

Online-Funktionen - Diagnose und Logging (Seite 257)

So erreichen Sie diese Funktion

1. Selektieren Sie im Navigationsbereich das Objekt "Alle Baugruppen".
2. Wählen Sie den Menübefehl "Einfügen" > "Baugruppe".
3. Nehmen Sie die folgenden Einstellungen vor.

<table>
<tr><th>Parameter</th><th>Bedeutung</th></tr>
<tr><td>Produkttyp</td><td>Produkttyp, der beim Anlegen einer neuen Baugruppe verwendet wird.
SCALANCE S
SCALANCE M
SOFTNET Konfiguration (SOFTNET Security Client, VPN Gerät, NCP VPN-Client)</td></tr>
<tr><td>Baugruppe</td><td>Je nach Auswahl des Produkttyps können Sie hier den Baugruppentyp angeben, der beim Anlegen einer neuen Baugruppe verwendet wird.
Wählen Sie die Option "NCP VPN-Client für Android", um ein VPN-Client-Gerät einzufügen, das stellvertretend für ein Gerät mit installierter Software NCP Secure VPN Client for Android steht.
Wählen Sie die Option "VPN-Gerät", um ein VPN-Client-Gerät einzufügen, welches stellvertretend für ein Gerät von einem anderen Hersteller steht.
Hinweis
Die ausgeleitete Konfigurationsdatei stellt lediglich eine Hilfe zur Konfiguration der VPN-Verbindung dar, ist aber keine Garantie für eine Kompatibilität mit Produkten anderer Hersteller.</td></tr>
<tr><td>Firmwarerelease</td><td>Für die SCALANCE S Baugruppen sowie für den SOFTNET Security Client können hier die Firmware- / Softwarestände angegeben werden.</td></tr>
<tr><td>Name der Baugruppe</td><td>Frei wählbarer Name der Baugruppe.</td></tr>
<tr><td>MAC-Adresse</td><td>Eingabe der MAC-Adresse der Baugruppe.</td></tr>
<tr><td>IP-Adresse (ext.)</td><td>IP-Adresse für die externe Schnittstelle.
Die IP-Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind, z. B. 141.80.0.16</td></tr>
<tr><td>Subnetzmaske (ext.)</td><td>Wertebereich für Subnetzmaske. Wird entsprechend der eingegebenen IP-Adresse vorgeschlagen.
Die Subnetzmaske besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 255.255.0.0</td></tr>
<tr><td>Schnittstellenrouting Extern/Intern</td><td>Auswahl der Betriebsart für die Security-Baugruppe. Für SCALANCE S stehen folgende Betriebsarten zur Verfügung:
• Bridge-Modus
• Routing-Modus
Wenn Sie den Routing-Modus auswählen, müssen Sie eine IP-Adresse und eine Subnetzmaske für die interne Schnittstelle der Security-Baugruppe projektieren.</td></tr>
<tr><td>IP-Adresse (int.)
nur anzugeben, wenn Routing-Modus aktiviert</td><td>IP-Adresse für die interne Schnittstelle.
Die IP-Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 141.90.10.10</td></tr>
</table>

Parameter	Bedeutung
Subnetzmaske (int.) nur anzugeben, wenn Routing-Modus aktiviert	Wertebereich für Subnetzmaske. Die Subnetzmaske wird entsprechend der eingegebenen IP-Adresse vorgeschlagen. Die Subnetzmaske besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 255.255.0.0
Auswahl speichern	Wenn Sie diese Funktion aktivieren, wird Ihre derzeit eingestellte Konfiguration in die Standard-Initialisierungswerte übernommen. Beim Einfügen von neuen Baugruppen wird dann nicht mehr der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" geöffnet, sondern gleich eine Baugruppe entsprechend den festgelegten Einstellungen in das Projekt eingefügt. Um diese Funktion wieder aufzuheben und einen anderen Baugruppentyp auszuwählen, müssen Sie diese Funktion unter folgendem Menüpfad deaktivieren: "Projekt" > "Eigenschaften..." > "Standard-Initialisierungswerte"

Hinweis

Zusätzliche Einstellungen

Weitere Schnittstelleneinstellungen nehmen Sie im Register "Schnittstellen" der Baugruppeneigenschaften vor. Informationen dazu finden Sie in Kapitel:

- Schnittstellen konfigurieren (Seite 94)

CPs in STEP 7 anlegen

CPs werden nur in STEP 7 angelegt. Sie erscheinen nach dem Anlegen und der Festlegung als Security-Baugruppe in den STEP 7 Baugruppeneigenschaften in der Liste der konfigurierten Baugruppen in SCT. Die Adressdaten werden aus STEP 7 übernommen und können in SCT nicht geändert werden.

Siehe auch

Parameter im Inhaltsbereich (Seite 91)

Wertebereiche IP-Adresse, Subnetzmaske und Adresse des Netzübergangs (Seite 273)

MAC-Adresse (Seite 274)

3.1 Parameter im Inhaltsbereich

So erreichen Sie die Ansicht

Selektieren Sie im Navigationsbereich das Objekt "Alle Baugruppen".

Für CPs können ausschließlich die Inhalte der Spalte "Kommentar" bearbeitet werden.

Folgende Eigenschaften der Baugruppen werden spaltenweise angezeigt:

Eigenschaft/Spalte	Bedeutung	Kommentar/Auswahl
Nr.	Fortlaufende Baugruppennummer	wird automatisch vergeben
Name	Eindeutige Baugruppenbenennung	frei wählbar
Typ	Gerätetyp	**Hinweis** Für Geräte vom Typ "SOFTNET Security Client" sowie "NCP-VPN-Client für Android" existiert kein Eigenschaftsdialog. Für VPN-Geräte können Sie in den Baugruppeneigenschaften ausschließlich die Dateitypen der zu exportierenden Konfigurationsdateien anpassen.
IP-Adresse ext.	IP-Adresse, über die das Gerät im externen Netz erreichbar ist, z. B. zum Laden der Konfiguration	Im Netzverbund passende Vergabe.
Subnetzmaske ext.	Subnetzmaske für die externe IP-Adresse	Im Netzverbund passende Vergabe.
IP-Adresse int.	IP-Adresse, über die das Gerät im internen Netz erreichbar ist, wenn es als Router konfiguriert ist	Im Netzverbund passende Vergabe. Das Eingabefeld ist nur dann editierbar, wenn der Routing-Modus aktiviert ist.
Subnetzmaske int.	Subnetzmaske für die interne IP-Adresse	Im Netzverbund passende Vergabe. Das Eingabefeld ist nur dann editierbar, wenn der Routing-Modus aktiviert ist.
Standard-Router	IP-Adresse des Standard-Routers	Im Netzverbund passende Vergabe.
MAC-Adresse	Hardware-Adresse der Baugruppe	Die MAC-Adresse ist auf dem Baugruppengehäuse aufgedruckt.
Kommentar	Information zur Baugruppe und das durch die Baugruppe geschützte Subnetz	frei wählbar

Adressparameter für SCALANCE S / M verändern

Für SCALANCE S / M Baugruppen können einige Adressparameter im Inhaltsbereich eingegeben und verändert werden.

Bedeutung der Adressparameter für CPs



Für die CPs werden die folgenden Adressen aus STEP 7 angezeigt:

Feld in SCT	CP x43-1 Adv.	CP 1628
IP-Adresse ext.	IP-Adresse Gigabit	IP-Adresse IE (Industrial Ethernet)
Subnetzmaske ext	Subnetzmaske Gigabit	Subnetzmaske IE

Feld in SCT	CP x43-1 Adv.	CP 1628
IP-Adresse int.	IP-Adresse PROFINET	Wird nicht angezeigt
Subnetzmaske int.	Subnetzmaske PROFINET	Wird nicht angezeigt
Standard-Router	In STEP 7 projektierter Standard-Router	In STEP 7 projektierter Standard-Router
MAC-Adresse	MAC-Adresse Gigabit (falls projektiert)	MAC-Adresse IE (falls projektiert)

Ebenfalls angezeigt werden die Adressdaten im Register "Schnittstellen".

Dynamisch vergebene IP-Adresse



Ist in STEP 7 projektiert, dass die IP-Adresse dynamisch vergeben werden soll, wird dies in SCT je nach Einstellungen folgendermaßen dargestellt:

Tabelle 3- 1 Gigabit-Schnittstelle

Betriebsart in STEP 7	IP-Adresse ext. / Subnetzmaske ext. (Felder in SCT)
IP-Adresse von einem DHCP-Server beziehen	dynamisch

Tabelle 3- 2 PROFINET-Schnittstelle

Betriebsart in STEP 7	IP-Adresse int. / Subnetzmaske int. (Felder in SCT)
IP-Adresse von einem DHCP-Server beziehen	dynamisch
IP-Adresse im Anwenderprogramm einstellen	
IP-Adresse auf anderem Weg einstellen	

3.2 Schnittstellen konfigurieren

3.2.1 Übersicht Anschlussmöglichkeiten



Unterstützte Anschlussmöglichkeiten

Jede Security-Baugruppe besitzt eine bestimmte Anzahl an Ports, an die die Netzwerkteilnehmer angeschlossen werden können. Abhängig von der zugehörigen Schnittstelle werden die Netzwerkteilnehmer unterschiedlich behandelt.

Security-Baugruppe	Schnitt-stelle	MAC-Adresse der Schnittstelle*	Port der Schnitt-stelle	Port-Typ	MAC-Adresse des Ports*
SCALANCE S602 / S612 / S613	Extern	MAC-Adresse (siehe Aufdruck)	P1	Fest eingebaute RJ-45 Buchse (Kupfer)	MAC-Adresse + 2
	Intern	MAC-Adresse + 1	P2	Fest eingebaute RJ-45 Buchse (Kupfer)	MAC-Adresse + 3
SCALANCE S623	Extern	MAC-Adresse (siehe Aufdruck)	P1	Fest eingebaute RJ-45 Buchse (Kupfer)	MAC-Adresse + 3
	Intern	MAC-Adresse + 1	P2	Fest eingebaute RJ-45 Buchse (Kupfer)	MAC-Adresse + 4
	DMZ	MAC-Adresse + 2	P3	Fest eingebaute RJ-45 Buchse (Kupfer)	MAC-Adresse + 5
SCALANCE S627-2M	Extern	MAC-Adresse (siehe Aufdruck)	P1	Fest eingebaute RJ-45 Buchse (Kupfer)	MAC-Adresse + 3
			P4	Medienmodulport (Kupfer/LWL)	MAC-Adresse + 4
			P5	Medienmodulport (Kupfer/LWL)	MAC-Adresse + 5
	Intern	MAC-Adresse + 1	P2	Fest eingebaute RJ-45 Buchse (Kupfer)	MAC-Adresse + 6
			P6	Medienmodulport (Kupfer/LWL)	MAC-Adresse + 7
			P7	Medienmodulport (Kupfer/LWL)	MAC-Adresse + 8
	DMZ	MAC-Adresse + 2	P3	Fest eingebaute RJ-45 Buchse (Kupfer)	MAC-Adresse + 9

* Beim Betrieb im Bridge-Modus ist immer die aufgedruckte MAC-Adresse an der externen und an der internen Schnittstelle gültig.

Die MAC-Adressen der Schnittstellen werden für alle Dienste außer LLDP verwendet.

Die MAC-Adressen der Ports werden zur Topologieerkennung mit LLDP (nur für Baugruppen im Routing-Modus) verwendet.

Hinweis

Die Ethernet-Schnittstellen dürfen beim Anschluss an das Kommunikationsnetzwerk nicht verwechselt werden:

- Schnittstelle X1 - Extern
  Rote Markierung = ungeschützter Netzwerkbereich;
- Schnittstelle X2 - Intern
  Grüne Markierung = durch SCALANCE S geschütztes Netzwerk;
- Schnittstelle X3 - DMZ (universelle Netzwerkschnittstelle)
  Gelbe Markierung = ungeschützter Netzwerkbereich oder durch SCALANCE S geschützter Netzwerkbereich.

Beim Vertauschen der Schnittstellen verliert das Gerät seine Schutzfunktion.

Funktionen der DMZ-Schnittstelle S62x

Eine Demilitarisierte Zone (DMZ) wird genutzt, wenn Dienste für ein externes Netz bereitgestellt werden sollen und das interne Netz, das Daten für diese Dienste liefert, von dem externen Netz entkoppelt sein soll. In der DMZ können z. B. Terminal-Server stehen, auf denen Wartungs- und Diagnose-Programme installiert sind, die definierte Zugriffe auf bestimmte Systeme im sicheren Netz erlauben. Zugriff haben nur zugelassene Benutzer oder Clients aus dem unsicheren Netz oder per VPN angeschlossene Clients. Die Firewall-Regeln können so projektiert werden, dass vom Internet Zugriffe auf Geräte in der DMZ aber nicht auf das interne Netz möglich sind. Für erhöhten Schutz können erlaubte Zugriffe ausschließlich auf VPN-Datenverkehr eingeschränkt werden. Eine exemplarische Konfiguration, in welcher die DMZ-Schnittstelle zur Einrichtung einer DMZ genutzt wird, wird im Kapitel "4.2 SCALANCE S als Firewall zwischen externem Netz und DMZ" des Handbuchs "SIMATIC NET Industrial Ethernet Security - Security einrichten" durchgeführt. Um auch Geräten in der DMZ eine dynamische IP-Adresse zuweisen zu können, kann auf der DMZ-Schnittstelle ein DHCP-Server aktiviert werden. Allerdings muss in einem solchen Anwendungsfall dafür gesorgt werden, dass die Geräte in der DMZ per DHCP immer die gleiche IP-Adresse bekommen, da diese IP-Adressen bei der Firewall-Konfiguration zu benutzen sind. D.h. bei der DHCP-Projektierung darf nicht die dynamische Adressvergabe, sondern nur die statische Adressvergabe anhand der MAC-Adresse oder anhand der Client-ID verwendet werden.

Die DMZ-Schnittstelle kann als VPN-Endpunkt genutzt werden. In Verbindung mit einem DSL-Modem wird die DMZ-Schnittstelle dann im PPPoE-Modus betrieben bzw. in Verbindung mit einem vorgeschalteten DSL-Router mit statischer IP-Adresse. Eine exemplarische Konfiguration, in welcher die DMZ-Schnittstelle zum Fernzugriff über einen VPN-Tunnel genutzt wird, wird im Kapitel "5.2 VPN-Tunnel zwischen SCALANCE S623 und SCALANCE S612" des Handbuchs "SIMATIC NET Industrial Ethernet Security - Security einrichten" durchgeführt.

Medienmodulports der externen und internen Schnittstelle S627-2M

Zusätzlich zu den Funktionen des SCALANCE S623 besitzt der SCALANCE S627-2M zwei Medienmodulslots, in die jeweils ein elektrisches oder optisches 2-Port-Medienmodul eingesetzt werden kann. Dadurch wird die externe und die interne Schnittstelle um jeweils bis zu zwei Ports erweitert. Wird für eine Schnittstelle das Medienmodul "MM992-2SFP" verwendet, können in das Medienmodul dieser Schnittstelle bis zu zwei elektrische oder optische SFP-Transceiver (Small Form-factor Pluggable Transceiver) eingesetzt werden. Die zusätzlichen Ports können für die Anbindung der externen und internen Schnittstelle des SCALANCE S627-2M an MRP-/HRP-Ringe verwendet werden.

Die Medienmodulports sind mit dem fest eingebauten Port der jeweiligen Schnittstelle über einen Switch-Baustein verbunden. Zwischen den über einen Switch-Baustein verbundenen Ports ist keine Firewall-Funktionalität (Ebene 2 / Ebene 3) gegeben. Alle über einen Switch-Baustein verbundenen Ports sind über dieselbe IP-Adresse erreichbar.

Funktionen der einzelnen Schnittstellen

Folgende Funktionen können auf den einzelnen Schnittstellen genutzt werden:

Funktion	Grün (internal)	Rot (external)	Gelb (DMZ)
Statische IP-Adresse	x	x	x
WAN-Zugang mit DSL-Router	-	x	x
WAN-Zugang mit DSL-Modem (PPPoE, dynamische IP-Adresse vom ISP)	-	x (Wenn nicht auf gelber Schnittstelle)	x (Wenn nicht auf roter Schnittstelle)
Bridge-Modus	x		-
Routing-Modus	x	x	x
Ghost-Modus S602 ≥V3.1	-	x	-
DHCP-Server	x	-	x
Endpunkt einer VPN-Tunnelverbindung (mit DSL-Modem und DSL-Router)	-	x	x
MRP-/HRP-Client (im Routing-Modus, Ringports auf den Medienmodulen) S627-2M	x	x	-
LLDP (im Routing-Modus) S≥V4.0	x	x	x
Passive Listening (im Routing-Modus, wenn Medienmodule gesteckt) S627-2M	x	x	-

x wird unterstützt

- wird nicht unterstützt

Duplex-Verfahren

Für einen Port kann eines von zwei Duplex-Verfahren ausgewählt werden:

- Halbduplex: Die Security-Baugruppe kann zu einem Zeitpunkt entweder Daten empfangen oder senden.
- Vollduplex: Die Security-Baugruppe kann zu einem Zeitpunkt gleichzeitig Daten empfangen und senden.

Hinweis

Duplex-Verfahren und Übertragungsgeschwindigkeit bei optischen Ports S627-2M

Für Ports mit dem Port-Typ "Optisch" ist der Port-Modus durch das verwendete Medienmodul bzw. durch den verwendeten SFP fest vorgegeben und kann nicht angepasst werden.

3.2.2 Schnittstellen



SCA. M

So erreichen Sie diese Funktion:

1. Markieren Sie die zu bearbeitende Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Schnittstellen".

Schnittstellenrouting - Auswahlmöglichkeiten SCA. S

Wenn sich die SCALANCE S Baugruppe in keiner VPN-Gruppe und in keiner Redundanzbeziehung befindet, kann das Schnittstellenrouting in diesem Feld verändert werden. Die Auswahl gilt für das Schnittstellenrouting zwischen externer und interner Schnittstelle. Die DMZ-Schnittstelle (nur SCALANCE S623 und SCALANCE S627-2M) wird immer im Routing-Modus angebunden.

Bridge-Modus	Für den Betrieb in flachen Netzen. Externe und interne Schnittstelle befinden sich im selben IP-Subnetz. Für S623 / S627-2M: Externe und interne Schnittstelle befinden sich im selben IP-Subnetz, DMZ-Schnittstelle befindet sich in einem anderen IP-Subnetz oder ist deaktiviert.
Routing-Modus	Alle Schnittstellen befinden sich in verschiedenen IP-Subnetzen. **Hinweis** Wenn Sie für die SCALANCE S Baugruppe den Routing-Modus aktiviert haben, können keine MAC-Firewall-Regeln definiert werden.
Ghost-Modus S602 ≥V3.1	Im Betrieb übernimmt die SCALANCE S Baugruppe für die externe Schnittstelle die IP-Adresse des Teilnehmers, der an der internen Schnittstelle der SCALANCE S Baugruppe angeschlossen ist. Die für die externe Schnittstelle anzugebenden IP-Adressdaten dienen lediglich dem Projektierungsladen vor dem Betrieb im Ghost-Modus. **Hinweis** Der Ghost-Modus ist im Register "Schnittstellen" nur auswählbar, wenn sich das Projekt im Erweiterten Modus befindet.

Projektierung der Schnittstellen

Wenn die Schnittstelle einer Baugruppe projektiert werden soll, muss diese über das Kontrollkästchen "Schnittstelle aktivieren" aktiviert sein. Legen Sie die IP-Adressangaben pro Schnittstelle sowie Einstellungen einzelner Ports (nur für SCALANCE S ab V3) fest. Für die Zuweisung einer IP-Adresse stehen Ihnen für die externe Schnittstelle und für die DMZ-Schnittstelle (nur SCALANCE S623/S627-2M) folgende Zuweisungsmodi zur Verfügung:

- Statische IP-Adresse mit Subnetzmaske
- Adresszuweisung über PPPoE S≥V3.0

  Die interne Schnittstelle sowie die Tunnel-Schnittstelle (nur für SCALANCE S612/S623/S627-2M ab V4) kann nur über eine statische IP-Adresse projektiert werden.

Wenn durch die Projektierung einer NAT-/NAPT-Regel für eine SCALANCE S Baugruppe Alias-IP-Adressen an einer Schnittstelle registriert wurden, werden diese im Feld "Alias-IP-Adressen" angezeigt.

Hinweis

Externe Schnittstelle und DMZ-Schnittstelle (nur SCALANCE S623/S627-2M) als Internetzugang

Der gleichzeitige Betrieb von PPPoE an der externen Schnittstelle und an der DMZ-Schnittstelle (Dual-ISP) ist nicht möglich.

Bedeutung der Tunnel-IP-Adresse S≥V4.0 ~~S602~~

Wenn Sie die Funktion "NAT/NAPT im VPN-Tunnel" benutzen, müssen Sie eine Tunnel-IP-Adresse für die Security-Baugruppe vergeben. Damit wird die Erreichbarkeit der Security-Baugruppe über den VPN-Tunnel sichergestellt und eine Konfigurations- und Diagnosemöglichkeit gewährleistet. Die projektierte Tunnel-IP-Adresse kann mit Hilfe entsprechender NAT-/NAPT-Regeln um Alias-Tunnel-IP-Adressen ergänzt werden. Die Subnetzmaske ist mit 32 Bit fest für die Tunnel-IP-Adresse vorgegeben und kann nicht verändert werden. Die Tunnel-IP-Adresse kann nur projektiert werden, wenn folgende Voraussetzungen erfüllt sind:

- Die Security-Baugruppe befindet sich in einer VPN-Gruppe.
- Das Projekt befindet sich im Erweiterten Modus.

Weitere Informationen zur Adressumsetzung mit NAT/NAPT in VPN-Tunneln finden Sie in folgendem Kapitel:
Adressumsetzung mit NAT/NAPT in VPN-Tunneln (Seite 182)

Point to Point Protocol over Ethernet (PPPoE) S≥V3.0

Um einen Internet-/WAN-Anschluss direkt über ein DSL-Modem zu ermöglichen, erfolgt die Zuweisung der IP-Adresse an der externen Schnittstelle bzw. an der DMZ-Schnittstelle über PPPoE. Bei PPPoE handelt es sich um ein Einwahlprotokoll zum Bezug von IP-Adressen von einem Internet Service Provider (ISP). SCALANCE S wird dabei im Routing-Modus betrieben.

Zur Verwendung dieser IP-Adresszuweisungsmethode geben Sie Angaben zum ISP im Register "Internetverbindung" an. Die IP-Adresse, die Subnetzmaske, der Standard-Router sowie der DNS-Server der Schnittstelle werden dann vom ISP vorgegeben.

Hinweis

Ein projektierter Standard-Router wird bei Verwendung von PPPoE nicht berücksichtigt. Dieser wird der Baugruppe dynamisch vom ISP vorgegeben.

Hinweis

Keine Netzwerkkomponenten zwischen SCALANCE S und DSL-Modem

Wenn die Schnittstelle einer SCALANCE S Baugruppe über PPPoE betrieben wird, dürfen sich zwischen dieser Schnittstelle und dem angeschlossenen DSL-Modem keine weiteren Netzwerkkomponenten befinden, da die Einwahldaten des Internet Service Providers auf dieser Strecke ggf. unverschlüsselt übertragen werden. Bei Verwendung des Authentifizierungsprotokolls "CHAP" werden die Daten verschlüsselt übertragen.

Porteinstellungen S≥V3.0

<table>
<tr><th>Spalte</th><th colspan="3">Bedeutung</th></tr>
<tr><td>Port-ID</td><td colspan="3">Automatisch vergebene ID für den Port der Schnittstelle.</td></tr>
<tr><td>Port-Typ</td><td colspan="3">Physikalische Eigenschaft des Ports (Kupfer/LWL)</td></tr>
<tr><td rowspan="6">Port-Modus</td><td>Autonegotiation</td><td colspan="2">Die Übertragungsgeschwindigkeit und das Duplex-Verfahren werden automatisch zwischen IEEE 802.3-konformen Ports ausgehandelt.
Hinweis
Nur wenn Autonegotiation ausgewählt ist, wird eine Übertragungsgeschwindigkeit von 1000 MBit/s sowie die Autocrossing-Funktion unterstützt.</td></tr>
<tr><td>10 MBit/s, half- und full-duplex</td><td colspan="2">Übertragungsgeschwindigkeit von 10 MBit/s</td></tr>
<tr><td>100 MBit/s, half- und full-duplex</td><td colspan="2">Übertragungsgeschwindigkeit von 100 MBit/s</td></tr>
<tr><td>Long Distance Signalling (LDS)</td><td colspan="2">Die Übertragungsgeschwindigkeit und das Duplex-Verfahren werden automatisch zwischen BroadR-Reach-konformen Ports ausgehandelt.</td></tr>
<tr><td>Aus (nur externer Port oder DMZ-Port bei SCALANCE S623 und SCALANCE S627-2M)</td><td colspan="2">Der Port wird deaktiviert.</td></tr>
<tr><td colspan="3">Hinweis S627-2M
Ports von Medienmodulen, die als Übertragungsmedium Lichtwellenleiter verwenden, arbeiten stets mit dem Vollduplex-Verfahren und maximaler Übertragungsgeschwindigkeit. Der Port-Modus von Ports optischer Medienmodule kann deshalb nicht projektiert werden.</td></tr>
<tr><td rowspan="2">S≥V4.0
LLDP-Modus (im Routing-Modus)</td><td>RxTx</td><td>LLDP-Telegramme senden und empfangen</td><td rowspan="2">Nähere Informationen zu LLDP finden Sie in folgendem Kapitel:
LLDP (Seite 107)</td></tr>
<tr><td>Off</td><td>LLDP-Telegramme empfangen</td></tr>
<tr><td>S627-2M
MRP-Port (im Routing-Modus für die Medienmodulports der externen und internen Schnittstelle)</td><td colspan="3">Anzeige, ob die Medienmodulports der Schnittstelle an einen MRP-Ring angebunden sind. Ist dies der Fall, werden die Zeichenketten "RingportOne" und "RingportTwo" in den Tabellenzeilen der Medienmodulports angezeigt. Für die Ports mit der Port-ID "X1 P1" und "X2 P1" wird standardmäßig die Zeichenkette "None" angezeigt, da diese nicht an einem MRP-Ring beteiligt sein können.
Allgemeine Informationen zu Medienredundanz mit MRP finden Sie in folgendem Kapitel:
Medienredundanz mit MRP/HRP (Seite 108)
Informationen zur Projektierung von MRP für die Security-Baugruppe finden Sie in folgendem Kapitel:
MRP/HRP für die Security-Baugruppe projektieren (Seite 109)</td></tr>
</table>

Spalte	Bedeutung
S627-2M HRP-Port (im Routing-Modus für die Medienmodulports der externen und internen Schnittstelle)	Anzeige, ob die Medienmodulports der Schnittstelle an einen HRP-Ring angebunden sind. Ist dies der Fall, werden die Zeichenketten "RingportOne" und "RingportTwo" in den Tabellenzeilen der Medienmodulports angezeigt. Für die Ports mit der Port-ID "X1 P1" und "X2 P1" wird standardmäßig die Zeichenkette "None" angezeigt, da diese nicht an einem HRP-Ring beteiligt sein können. Allgemeine Informationen zu Medienredundanz mit HRP finden Sie in folgendem Kapitel: Medienredundanz mit MRP/HRP (Seite 108) Informationen zur Projektierung von HRP für die Security-Baugruppe finden Sie in folgendem Kapitel: MRP/HRP für die Security-Baugruppe projektieren (Seite 109)
Kommentar	Frei wählbarer Kommentar

Konfiguration von Medienmodulen S627-2M

Klicken Sie auf die Schaltfläche "Medienmodul konfigurieren...", um den Dialog zur Konfiguration des Medienmoduls für die zugehörige Schnittstelle aufzurufen.

Zur Auswahl stehen die beiden folgenden Konfigurationsmodi:

- "Automatisch" (Standardeinstellung): Das verwendete Medienmodul wird im Betrieb automatisch erkannt. Der Port-Modus wird für beide Ports auf "Auto-Negotiation" eingestellt.
- "Manuell": Wählen Sie den verwendeten Medienmodultyp aus der Klappliste "Modultyp" aus. Wenn Sie den Medienmodultyp "MM992-2SFP" auswählen, können Sie über die beiden Klapplisten "SFP-Typ" die gewünschten Stecktransceiver (SFPs) auswählen. Für Ports mit dem Port-Typ "Kupfer" können Sie die Übertragungsgeschwindigkeit sowie das Duplex-Verfahren über den Port-Modus manuell festlegen. Für Ports mit dem Port-Typ "Optisch" ist der Port-Modus durch das verwendete Medienmodul bzw. den verwendeten SFP fest vorgegeben und kann nicht angepasst werden.

Siehe auch

Besonderheiten des Ghost-Modus (Seite 111)

Übersicht Anschlussmöglichkeiten (Seite 94)

Konfigurationsdaten für SCALANCE M Baugruppen (Seite 220)

3.2.3 Internetverbindung



So erreichen Sie diese Funktion:

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Internetverbindung".

Bedeutung

Wenn für eine der Schnittstellen der Security-Baugruppe eine Verbindung über PPPoE eingestellt ist, nehmen Sie in diesem Register Einstellungen zum Internet Service Provider (ISP) vor.

Tabelle 3- 3 Einstellungen zum ISP-Account

Funktion	Beschreibung
Benutzername	Geben Sie den Namen zur Anmeldung beim ISP-Account ein.
Passwort	Geben Sie das Passwort zur Anmeldung beim ISP-Account ein.
Passwort wiederholen	Geben Sie das Passwort zur Anmeldung beim ISP-Account erneut ein.
Authentifizierung	Wählen Sie keines oder eines der folgenden Authentifizierungsprotokolle: • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) **Hinweis** Beide Kommunikationspartner müssen dasselbe Authentifizierungsverfahren verwenden, ansonsten kann keine Verbindung aufgebaut werden.

Tabelle 3- 4 Regeln für Benutzernamen und Passwörter

<table>
<tr><td>Erlaubte Zeichen</td><td>Erlaubt sind folgende Zeichen des Zeichensatzes ANSI X 3.4-1986:
0123456789
A...Z a...z
!#$%&()"*'+`,-./:;<=>?@ [\]_{|}~^</td></tr>
<tr><td>Länge des Benutzernamens</td><td>1 ... 255 Zeichen</td></tr>
<tr><td>Länge des Passworts</td><td>1 ... 31 Zeichen</td></tr>
</table>

Tabelle 3- 5 Einstellungen zur Verbindung

Funktion	Beschreibung
Dauerhafte Verbindung	Ständige Internetverbindung. Nach einer Trennung durch den Provider wird die Verbindung automatisch wieder hergestellt, auch wenn aktuell keine Pakete gesendet werden sollen.
On-Demand-Verbindung	Die Internetverbindung wird automatisch aufgebaut, wenn Pakete ins Internet gesendet werden sollen. In dieser Einstellung sind Verzögerungen beim Versenden der Pakete möglich.
Zwangstrennung (nur bei Einstellung "Dauerhafte Verbindung")	Der Provider trennt nach einem bestimmten Zeitraum die Internetverbindung automatisch. Tragen Sie im Feld "Zwangstrennung" eine Uhrzeit ein, trennt die Security-Baugruppe zu diesem Zeitpunkt von sich aus die Internetverbindung. Damit kann eine Trennung der Internetverbindung von Seiten des Providers unter Umständen verschoben werden. Eine selbst initiierte Zwangstrennung ist nur bei einer bestehenden dauerhaften Verbindung möglich. Erlaubte Eingaben: 00:00 ... 23:59
Maximale Leerlaufzeit (nur bei Einstellung "On-Demand-Verbindung")	Werden innerhalb einer bestimmten Zeit keine Pakete gesendet, wird die Internetverbindung automatisch getrennt. Geben Sie im Feld "Maximale Leerlaufzeit" die Zeit in Sekunden ein, nach der die Verbindung getrennt werden soll. Erlaubte Werte: 10 … 3600.

Adressumsetzung in das PPPoE-Netz projektieren

Das Kontrollkästchen "Erlaube NAT von intern in das PPPoE-Netz" ist nur verfügbar, wenn sich das Projekt nicht im erweiterten Modus befindet. Wenn Sie das Kontrollkästchen aktivieren, wird durch SCT eine NAT-Regel angelegt, mit welcher die Quell-IP-Adressen aller Teilnehmer im internen Netz auf die Baugruppen-IP-Adresse im PPPoE-Netz umgesetzt werden. Diese NAT-Regel sowie die zugehörige Firewall-Regel ist nach dem Aktivieren des Kontrollkästchens im erweiterten Modus sichtbar.

3.2.4 Dynamisches DNS (DDNS)



Bedeutung

Mit dynamischem DNS können Sie mit einem fest definierten Namen (FQDN) auf eine sich ständig ändernde IP-Adresse zugreifen. Dies ist notwendig, wenn Sie z. B. auf einen Server zugreifen möchten, der über eine öffentliche, sich ändernde IP-Adresse erreichbar ist.

Funktionsweise

Die Security-Baugruppe meldet einem Anbieter für dynamisches DNS (z. B. DynDNS.org, no-ip.com) die aktuelle WAN-IP-Adresse, über die die Security-Baugruppe erreichbar ist. Der Provider sorgt dafür, dass DNS-Anfragen auf den FQDN der Security-Baugruppe mit der aktuellen WAN-IP-Adresse der Security-Baugruppe beantwortet werden.

Dynamisches DNS ist auf folgenden Schnittstellen zugelassen:

- Externe Schnittstelle
- DMZ-Schnittstelle

Dynamisches DNS einrichten - Voraussetzung

Voraussetzung:

- Bei einem Anbieter für dynamisches DNS ist ein Account angelegt und ein FQDN registriert.

Dynamisches DNS einrichten - Gehen Sie so vor:

1. Wählen Sie in den Baugruppeneigenschaften der Security-Baugruppe das Register "DNS".
2. Falls sich die Security-Baugruppe hinter einem DSL-Router oder einem DSL-Modem befindet, geben Sie die Adresse eines gültigen DNS-Servers an. Hierfür stehen Ihnen zwei Optionen zur Verfügung:

Option	Bedeutung
DNS-Serveradresse automatisch beziehen	Die Adresse des DNS-Servers kann über PPPoE automatisch bezogen werden, wenn die Security-Baugruppe über ein DSL-Modem mit dem Internet verbunden ist. Kann nur für die externe Schnittstelle und die DMZ-Schnittstelle eingestellt werden.
Folgende DNS-Serveradresse verwenden:	Geben Sie die Adresse des bevorzugten und des alternativen DNS-Servers manuell ein.

3. Aktivieren Sie das Kontrollkästchen "Service aktivieren" im Bereich "Primärer dyn. DNS-Dienst" und nehmen Sie die folgenden Einstellungen vor:

Einstellung	Bedeutung
Anbieter	Wählen Sie aus, bei welchem Anbieter Sie einen Account für dynamisches DNS eingerichtet haben.
Benutzerkonto beim Anbieter	Geben Sie den Benutzernamen ein, den Sie beim Anlegen des Accounts festgelegt haben.
Passwort beim Anbieter	Geben Sie das Passwort ein, das Sie beim Anlegen des Accounts festgelegt haben.
FQDN	Geben Sie den Hostnamen (z. B. mysecurity-device) und den Domainnamen (z. B. dyn-dns.org), der beim Anbieter registriert ist, durch einen Punkt getrennt ein. Ist im Register "VPN" ebenfalls ein FQDN eingetragen, müssen beide übereinstimmen.
IP-Adresswechsel auf DSL-Router überwachen	Ist die Security-Baugruppe über einen DSL-Router mit dem Internet verbunden, wird durch Aktivieren der Funktion der Prüf-IP-Dienst aktiviert. Die Security-Baugruppe sendet periodisch Anfragen zur Bestimmung der aktuellen IP-Adresse des DSL-Routers sowie zur Detektion eines IP-Adresswechsels auf dem DSL-Router. Die so bestimmte IP-Adresse wird bei jeder Änderungserkennung an den Anbieter gesendet.
Periode	Geben Sie an, in welchem Zyklus der Prüf-IP-Dienst aufgerufen wird. Erlaubte Werte: 10 … 1440 Minuten

4. Legen Sie für den Fall, dass der primäre Anbieter ausfällt, einen weiteren Anbieter im Register "Sekundärer dyn. DNS-Dienst" fest (optionale Einstellung).

Benutzerdefinierten Anbieter einrichten - Gehen Sie so vor:

Wählen Sie aus der Klappliste "Anbieter" den Eintrag "Benutzerdefiniert" aus und nehmen Sie zusätzlich folgende Eingaben vor:

Einstellung	Bedeutung
Anbieter-Aktualisierungs-URL	Geben Sie die jeweilige URL ein, die Sie von Ihrem Anbieter erhalten haben. Die Platzhaltertexte <FQDN> und <Current-WanIP> müssen hierbei an den zugehörigen Stellen der URL platziert werden.
Prüf-IP-Service-URL	Geben Sie die jeweilige URL ein, die Sie von Ihrem Anbieter erhalten haben.
Fehler bei Überprüfung des Server-Zertifikats ignorieren	Damit die Authentifizierungsdaten geschützt sind, wird das Zertifikat des Update-Servers standardmäßig überprüft. Schlägt die Prüfung des Zertifikates fehl, so wird die HTTPS-Verbindung beendet und die Account-Daten werden nicht übertragen. Wenn Sie das Kontrollkästchen aktivieren, wird die Funktion deaktiviert, z. B. wenn das Server-Zertifikat des dyn. DNS-Dienstes ungültig ist (z. B. abgelaufen). Es wird empfohlen, die Überprüfung nicht zu ignorieren und das Kontrollkästchen nicht zu aktivieren.

3.2.5 LLDP



Bedeutung

LLDP (Link Layer Discovery Protocol) ist ein Protokoll, das zur Erkennung von Netzwerktopologien verwendet wird. Ein LLDP-fähiges Gerät ist dazu in der Lage, in regelmäßigen Intervallen Informationen über sich selbst an Nachbargeräte zu senden und gleichzeitig Informationen von Nachbargeräten zu empfangen. Die empfangenen Informationen werden auf jedem LLDP-fähigen Gerät in einer LLDP-MIB-Datei gespeichert. Netzwerkmanagementsysteme können auf diese LLDP-MIB-Dateien mit Hilfe von SNMP zugreifen und damit die vorliegende Netzwerktopologie nachbilden.

Projektierbare Parameter

Das Ausmaß der Aktivität der Security-Baugruppe in Bezug auf LLDP kann im Register "Schnittstellen" der Baugruppeneigenschaften wie folgt projektiert werden:

- LLDP-Telegramme senden und empfangen (Standardeinstellung, "RxTx")
- LLDP-Telegramme empfangen ("Off")

3.2.6 Medienredundanz in Ringtopologien

3.2.6.1 Medienredundanz mit MRP/HRP



Bedeutung

Unter dem Begriff "Medienredundanz" werden verschiedene Verfahren zur Erhöhung der Verfügbarkeit von Industrial Ethernet-Netzen zusammengefasst, bei denen Geräte über mehrere Wege erreichbar sind. Dies kann über die Vermaschung von Netzen, Parallelschaltung von Übertragungswegen oder das Schließen einer Linientopologie zu einem Ring erfolgen.

Medienredundanzverfahren MRP und HRP

Medienredundanz innerhalb einer Ringtopologie gibt es bei SIMATIC NET-Produkten in den Verfahren MRP (Media Redundancy Protocol) und HRP (High Speed Redundancy Protocol).

Bei beiden Verfahren wird einer der Teilnehmer als Redundanz-Manager konfiguriert. Die anderen Teilnehmer sind Redundanz-Clients. SCALANCE S627-2M Baugruppen können ausschließlich die Rolle eines MRP- bzw. HRP-Clients einnehmen. Mit Testtelegrammen überprüft der Redundanz-Manager den Ring auf Unterbrechungsfreiheit. Die Redundanz-Clients leiten die Testtelegramme weiter. Wenn die Testtelegramme des Redundanz-Managers bei einer Unterbrechung des Rings nicht mehr am anderen Ringport des Redundanz-Managers ankommen, schaltet der Redundanz-Manager seine beiden Ringports durch und informiert die Redundanz-Clients umgehend über den Wechsel.

Die beiden Medienredundanzverfahren MRP und HRP arbeiten nach demselben Funktionsprinzip. Sie unterscheiden sich in der Zeitdauer, die SCALANCE X Switche als Redundanz-Manager zum Durchschalten ihrer Ringports benötigen:

- MRP: 200 ms
- HRP: 300 ms

Hinweis zum Einsatz von MRP und HRP

- MRP und HRP wird in Ringtopologien mit bis zu 100 Geräten unterstützt. Eine Überschreitung der Geräteanzahl kann zum Ausfall des Datenverkehrs führen.
- Es wird empfohlen, die beteiligten Ringports auf Full-Duplex und 100 Mbit/s einzustellen. Andernfalls kann es zum Ausfall des Datenverkehrs kommen.

Einsatzmöglichkeiten von MRP/HRP auf Medienmodulports

MRP/HRP wird ausschließlich auf den Medienmodulports des SCALANCE S627-2M unterstützt. Die folgende Tabelle zeigt die Einsatzmöglichkeiten von MRP/HRP auf den Medienmodulports eines SCALANCE S627-2M:

Ringports	Medienmodul 1		Medienmodul 2	
	P4	P5	P6	P7
MRP-Cient oder HRP-Client*	-	-	-	-
	Ring 1	Ring 1	-	-
	-	-	Ring 2	Ring 2
	Ring 1	Ring 1	Ring 2	Ring 2

* Die gleichzeitige Anbindung der Security-Baugruppe an einen internen und an einen externen Ring ist nur möglich, wenn mindestens eine der Schnittstellen als MRP-Client angebunden wird.

Bei zwei unterlagerten Ringen pro SCALANCE S Baugruppe ist Ebene 3 Kommunikation zwischen den Ringen möglich.

3.2.6.2 MRP/HRP für die Security-Baugruppe projektieren



Voraussetzungen

- Die Security-Baugruppe befindet sich im Routing-Modus.
- Für die Schnittstellen, die an Ringe angebunden werden sollen, sind Medienmodule projektiert.

So erreichen Sie diese Funktion

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "MRP/HRP".

Konfigurierbare Parameter

Parameter	Bedeutung	Auswahlmöglichkeiten
MRP/HRP-Schnittstellen	Auswahl der Schnittstelle, die an den MRP-/HRP-Ring angebunden werden soll.	• Extern • Intern
Medienredundanzrolle	Auswahl des Medienredundanzprotokolls bzw. Deaktivieren von Medienredundanz für die selektierte Schnittstelle.	• Nicht Teilnehmer des Rings • MRP-Client (Standard-Einstellung) • HRP-Client

Parameter	Bedeutung	Auswahlmöglichkeiten
Aktiviere 'passive listening'	Aktivieren Sie dieses Kontrollkästchen, wenn die ausgewählte Schnittstelle an Fremdnetze gekoppelt werden soll, in denen STP/RSTP (Spanning-Tree-Protocol/Rapid-Spanning-Tree-Protocol) eingesetzt wird.	• "Passive listening" aktivieren (Standardeinstellung) • "Passive listening" deaktivieren
MRP-Domain (nur bei Auswahl der Medienredundanzrolle "MRP-Client")	Mit Hilfe von MRP-Domains werden die Teilnehmer eines MRP-Rings festgelegt. Für die Schnittstellen aller Baugruppen, die an demselben MRP-Ring angebunden sein sollen, muss dieselbe MRP-Domain ausgewählt sein.	Standardmäßig ist für die externe Schnittstelle die vordefinierte MRP-Domain "mrpdomain-1" ausgewählt. Über die Schaltflächen "Hinzufügen...", "Bearbeiten..." und "Entfernen" können Sie neue MRP-Domains hinzufügen, die Namen bestehender MRP-Domains bearbeiten und bestehende MRP-Domains löschen.
Ringport 1 (nur bei Auswahl der Medienredundanzrolle "MRP-Client" oder "HRP-Client")	Bezeichnung des ersten Ringports der unter "Schnittstelle" ausgewählten Schnittstelle, wenn für diese die Medienredundanzrolle "MRP-Client" oder "HRP-Client" ausgewählt wurde.	-
Ringport 2 (nur bei Auswahl der Medienredundanzrolle "MRP-Client" oder "HRP-Client")	Bezeichnung des zweiten Ringports der unter "Schnittstelle" ausgewählten Schnittstelle, wenn für diese die Medienredundanzrolle "MRP-Client" oder "HRP-Client" ausgewählt wurde.	-
MRP-Teilnehmer (nur bei Auswahl der Medienredundanzrolle "MRP-Client")	Anzeige von Informationen zu allen Security-Baugruppen, die derselben MRP-Domain angehören wie die ausgewählte Schnittstelle.	-

Ergebnis

Sie haben die Security-Baugruppe über die ausgewählte Schnittstelle an den MRP-/HRP-Ring angebunden. Die Medienmodulports welcher Schnittstelle(n) an den MRP-/HRP-Ring angebunden sind, wird zusätzlich im Register "Schnittstellen" der Baugruppeneigenschaften angezeigt.

Konsistenzprüfung - diese Regel müssen Sie beachten

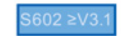
Berücksichtigen Sie bei Ihrer Eingabe die nachfolgend aufgeführte Regel:

- Die Namen von MRP-Domains dürfen ausschließlich aus Kleinbuchstaben, Zahlen und dem Zeichen "-" bestehen. Die Namen müssen mit einem Kleinbuchstaben oder einer Zahl beginnen und enden.

Siehe auch

Konsistenzprüfungen (Seite 63)

3.2.7 Besonderheiten des Ghost-Modus



Bedeutung

Im Ghost-Modus hat die Security-Baugruppe weder an der internen, noch an der externen Schnittstelle eine eigene IP-Adresse. Stattdessen bezieht die Security-Baugruppe zur Laufzeit die IP-Adresse für ihre externe Schnittstelle von einem Teilnehmer, der an der internen Schnittstelle der Security-Baugruppe angeschlossen ist und dessen IP-Adressparameter zum Projektierungszeitpunkt unbekannt sein können. Eine IP-Adressänderung des internen Teilnehmers und eine damit verbundene IP-Adressänderung an der externen Schnittstelle ist möglich. Da der interne Teilnehmer anhand seiner MAC-Adresse identifiziert wird, werden IP-Adressänderungen nur für die gelernte MAC-Adresse vorgenommen. An der internen Schnittstelle der Security-Baugruppe wird keine IP-Adresse projektiert bzw. bezogen.

Hinsichtlich der MAC-Adressen tauscht die Security-Baugruppe in allen an der externen Schnittstelle ausgehenden Datenpaketen (Antworten des internen Teilnehmers) die MAC-Adresse des internen Teilnehmers gegen die MAC-Adresse der Security-Baugruppe aus.

Ghost-Modus aktivieren - Gehen Sie so vor:

Voraussetzung: Der Ghost-Modus ist nur auswählbar, wenn sich das Projekt im Erweiterten Modus befindet.

1. Selektieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...".
3. Wählen Sie im Register "Schnittstellen" aus der Klappliste "Schnittstellenrouting Extern/Intern" den Eintrag "Ghost-Modus".

Projektierbare Baugruppeneigenschaften

Im Ghost-Modus sind die Baugruppeneigenschaften aus folgenden Registern projektierbar:

- Schnittstellen
- Firewall
- Zeitsynchronisierung
- Log-Einstellungen
- SNMP

Da im Ghost-Modus keine DNS-Server projektiert werden können, ist keine FQDN-Auflösung möglich.

Voraussetzung zur Erkennung eines internen Teilnehmers

Die Security-Baugruppe kann nur dann die IP-Adresse des internen Teilnehmers ermitteln, wenn der interne Teilnehmer von sich aus eine Datenkommunikation mit einem Kommunikationspartner des externen Netzes initiiert.
Die Security-Baugruppe bietet zudem während der Ermittlung der IP-Adresse keine Serverdienste an. Erst nachdem vom internen Teilnehmer Datenpakete an die Security-Baugruppe versendet wurden, kann die Security-Baugruppe Anfragen von extern beantworten.

Portbelegung für ein- und ausgehende Datenverbindungen

Da die externe Schnittstelle der Security-Baugruppe und der interne Teilnehmer die gleiche IP-Adresse besitzen, muss eine gezielte Adressierung der Netzkomponenten über die TCP-/UDP-Ports erfolgen. Die Ports sind deshalb entweder der Security-Baugruppe oder dem internen Teilnehmer zugeordnet. In den folgenden Tabellen sind die Zuordnungen der Ports zu den jeweiligen Geräten für eingehende und ausgehende Datenverbindungen dargestellt:

Tabelle 3- 6 Portbelegung für eingehende Verbindungen (von extern auf Security-Baugruppe)

Dienst	Port	Protokoll	Kommentar
Webdienste, Projektierungs- und Diagnosezugang	443	TCP	Der HTTPS-Port ist für den Projektierungs- und Diagnosezugang über das Security Configuration Tool immer aktiviert und nicht veränderbar.
SNMP	161	TCP UDP	Nach der Aktivierung von SNMP im Security Configuration Tool werden eingehende SNMP-Anfragen über UDP-Port 161 übertragen. Eine Übertragung über TCP-Port 161 ist ebenfalls möglich, um so beispielsweise den internen Teilnehmer erreichen zu können. **Hinweis** Nach dem Aktivieren von SNMP ist der SNMP-Port fest der Security-Baugruppe zugeordnet. Ist SNMP nicht aktiviert, kann mithilfe einer Firewall-Regel über SNMP auf den internen Teilnehmer zugegriffen werden.

Tabelle 3- 7 Portbelegung für ausgehende Verbindungen (von Security-Baugruppe nach extern)

Dienst	Port	Protokoll	Kommentar
Syslog	514	UDP	Wenn der Syslogdienst im Security Configuration Tool aktiviert ist, werden Syslog-Meldungen von der Security-Baugruppe über UDP-Port 514 übertragen. Diese Portbelegung ist nicht änderbar.
NTP	123	UDP	Wenn NTP-Server zur Zeitsynchronisierung genutzt werden, werden NTP-Anfragen über UDP-Port 123 übertragen. Diese Portbelegung ist nicht änderbar.

Erkennbare IP-Adressen und Subnetzmasken

Die Security-Baugruppe erkennt ausschließlich interne Teilnehmer, die IP-Adressen im Bereich der Netzklassen A, B oder C aufweisen. Die Subnetzmaske wird entsprechend der zugehörigen Netzklasse von der Security-Baugruppe ermittelt (siehe Tabelle "Netzklassen und zugehörige Subnetzmasken"). Damit die Subnetzmaske korrekt ermittelt werden kann, muss für den internen Teilnehmer ein Standard-Router eingetragen sein.

Teilnehmer mit IP-Adressen der Netzklassen D und E werden von der Security-Baugruppe abgelehnt.

Tabelle 3- 8 Netzklassen und zugehörige Subnetzmasken

Netzklasse	IP-Adressen		Subnetzmaske
	Untergrenze	Obergrenze	
A	0.0.0.0	127.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	Wird von Security-Baugruppe abgelehnt
E	240.0.0.0	255.255.255.255	Wird von Security-Baugruppe abgelehnt

Mengengerüst

Es wird maximal ein interner Teilnehmer von der Security-Baugruppe erkannt. Die Security-Baugruppe verhält sich bei mehreren internen Teilnehmern wie folgt:

- Das erste durch die Security-Baugruppe erkannte Gerät im internen Netz erhält Zugriff auf das externe Netzsegment, sofern die Firewall entsprechend konfiguriert ist.
- Der Datenverkehr von eventuell zusätzlich vorhandenen Teilnehmern im internen Netzbereich wird ausgehend auf Ebene 2 (MAC-Schicht) anhand der Absenderadresse geblockt.

Laden von Konfigurationen und Diagnose nach Inbetriebnahme

Nach dem Bezug einer IP-Adresse vom internen Teilnehmer besitzt die Security-Baugruppe an der externen Schnittstelle eine IP-Adresse, die von derjenigen IP-Adresse abweichen kann, mit welcher die Security-Baugruppe initial projektiert wurde. Für eine Änderung an der Konfiguration bzw. für Diagnosezwecke müssen Sie im Security Configuration Tool für die externe Schnittstelle die initial projektierte IP-Adresse durch diejenige ersetzen, die die Security-Baugruppe zur Laufzeit vom internen Teilnehmer bezogen hat.

Routinginformationen für hierarchische Netze am externen Port

Wenn sich an der externen Schnittstelle der Security-Baugruppe hierarchische Netze mit Subnetzübergängen befinden, muss die Security-Baugruppe die zugehörigen Routinginformationen vom internen Teilnehmer beziehen. Hierfür muss der interne Teilnehmer auf an ihn gerichtete ICMP-Anfragen antworten. Antworten auf ICMP-Broadcasts sind nicht notwendig.

Firewall projektieren 4

Bedeutung

Die Firewall-Funktionalität der Security-Baugruppen hat die Aufgabe, Netze und Stationen vor Fremdbeeinflussungen und Störungen zu schützen. Das bedeutet, dass nur bestimmte, vorher festgelegte Kommunikationsbeziehungen erlaubt werden. Nicht zugelassene Telegramme werden, ohne dass eine Antwort gesendet wird, von der Firewall verworfen.

Zur Filterung des Datenverkehrs können u. a. IP-Adressen, IP-Subnetze, Portnummern oder MAC-Adressen verwendet werden.

Die Firewall-Funktionalität kann für folgende Protokollebenen konfiguriert werden:

- IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
- Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3 (Layer 2)



Die Firewall kann für den verschlüsselten (IPsec-Tunnel) und den unverschlüsselten Datenverkehr eingesetzt werden.

Firewall-Regeln

Firewall-Regeln beschreiben, welche Pakete in welche Richtung erlaubt bzw. verboten werden. IP-Regeln wirken auf alle IP-Pakete ab Ebene 3. MAC-Regeln wirken nur auf Frames unterhalb Ebene 3.

Automatische Firewall-Regeln für STEP 7-Verbindungen



Für in STEP 7 projektierte Verbindungen werden automatisch Firewall-Regeln in SCT angelegt, die den Kommunikationspartner freigeben. Dabei werden die Aufbaurichtungen der Verbindungen beachtet.

Die Regeln sind nur im Erweiterten Modus sichtbar und können auch nur dort verändert werden.

Projektierung

Zu unterscheiden sind die beiden Bedienungssichten:

- Im Standard Modus greifen Sie auf einfache, vordefinierte Firewall-Regeln zurück. Sie können nur dienstspezifische Regeln freischalten. Die freigegebenen Dienste sind für alle Teilnehmer zulässig und es wird für die angegebene Richtung der volle Zugriff erlaubt.
- Im Erweiterten Modus können Sie detaillierte Firewall-Einstellungen vornehmen. Sie können für einen einzelnen Teilnehmer einzelne Dienste freischalten oder für den Teilnehmer alle Dienste für den Zugriff auf die Station bzw. das Netz freigeben.

  Zu unterscheiden sind im Erweiterten Modus die folgenden Firewall-Regeln bzw. -Regelsätze:

  – Lokale Firewall-Regeln sind jeweils einer Security-Baugruppe zugewiesen. Sie werden im Eigenschaftsdialog der Security-Baugruppen projektiert.

  – Globale Firewall-Regelsätze können einzelnen oder mehreren Security-Baugruppen gleichzeitig zugewiesen werden. Sie werden im Erweiterten Modus im Navigationsbereich des Security Configuration Tools angezeigt und global projektiert.

  – Benutzerspezifische IP-Regelsätze können einzelnen oder mehreren Security-Baugruppen gleichzeitig zugewiesen werden. Sie werden im Erweiterten Modus im Navigationsbereich des Security Configuration Tools angezeigt und global projektiert. SCALANCE S V4 (RADIUS): Benutzerspezifischen IP-Regelsätzen können neben einzelnen oder mehreren Benutzern auch einzelne oder mehrere Rollen zugewiesen sein.

Zusätzlich haben Sie die Möglichkeit, mit Hilfe von Dienst-Definitionen Firewall-Regeln kompakt und übersichtlich zu definieren. Dienst-Definitionen können in allen oben aufgeführten Regeltypen eingesetzt werden.

Firewall aktivieren

Die Firewall wird im Standard Modus durch Aktivieren des Optionskästchens "Firewall aktivieren" gesteuert. Deaktivieren Sie das Kontrollkästchen, werden die Firewall-Einstellungen, die Sie eingetragen haben, weiterhin in der Liste angezeigt, können jedoch nicht verändert werden. Befindet sich die Security-Baugruppe in einer VPN-Gruppe, ist das Kontrollkästchen standardmäßig aktiviert und kann nicht deaktiviert werden.

Logging-Einstellungen aktivieren

Im Standard Modus können Sie das Logging global im Register "Firewall" aktivieren. Damit werden Ihnen jedoch nicht alle Pakete angezeigt, welche die Firewall passieren.

Im Erweiterten Modus können Sie das Logging für jede einzelne Firewall-Regel aktivieren. Damit entfällt die Einschränkung bezüglich angezeigter Pakete aus dem Standard Modus.

Hinweis

Firewall von SCALANCE S627-2M

Die Medienmodulports des SCALANCE S627-2M sind mit dem fest eingebauten Port der jeweiligen Schnittstelle über einen Switch-Baustein verbunden. Zwischen den Ports der externen Schnittstelle untereinander sowie zwischen den Ports der internen Schnittstelle untereinander ist deshalb keine Firewall-Funktionalität (Layer 2 / Layer 3) gegeben.

4.1 CPs im Standard Modus

Paketfilter-Regeln aktivieren

Wenn Sie in STEP 7 für die CPs die Security-Funktion aktivieren, sind zunächst alle Zugriffe auf und über den CP zugelassen. Um einzelne Paketfilter-Regeln zu aktivieren, klicken Sie das Kontrollkästchen "Firewall aktivieren". Schalten Sie anschließend die gewünschten Dienste frei. Firewall-Regeln, die aufgrund einer Verbindungsprojektierung automatisch angelegt werden, haben Vorrang vor den hier eingestellten Diensten. Alle Teilnehmer haben über die von Ihnen freigegebenen Dienste Zugriff.

Detaillierte Firewall-Einstellungen im Erweiterten Modus

Im Erweiterten Modus können Sie Firewall-Regeln auf einzelne Teilnehmer beschränken. Um in den Erweiterten Modus zu wechseln, klicken Sie auf das Optionskästchen "Erweiterter Modus".

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sie können eine einmal vorgenommene Umschaltung in den Erweiterten Modus für das aktuelle Projekt nicht mehr rückgängig machen.

Firewall-Projektierung mit VPN

Befindet sich die Security-Baugruppe in einer VPN-Gruppe, ist standardmäßig das Kontrollkästchen "Ausschließlich getunnelte Kommunikation" aktiviert. Dies bedeutet, dass über die externe Schnittstelle keine Kommunikation am Tunnel vorbei gehen darf und nur verschlüsselter IPsec-Datentransfer zugelassen ist. Es wird automatisch die Firewall-Regel "Drop" > "Any" > "Extern" angelegt.

Deaktivieren Sie das Kontrollkästchen, dann sind die getunnelte Kommunikation und zusätzlich die in den anderen Auswahlboxen angewählten Kommunikationsarten zugelassen.

4.1.1 CP x43-1-Adv.

4.1.1.1 Voreinstellung der Firewall

Verhalten mit Voreinstellung

Die folgenden Diagramme zeigen die Standard-Einstellungen im Detail jeweils für den IP-Paketfilter und den MAC-Paketfilter, wenn das Kontrollkästchen "Firewall aktivieren" aktiviert ist und auch im Erweiterten Modus keine Regeln vorhanden sind. Das Verhalten kann durch das Anlegen von entsprechenden Firewall-Regeln im Erweiterten Modus geändert werden.

Standard-Einstellung für CP x43-1 Adv.

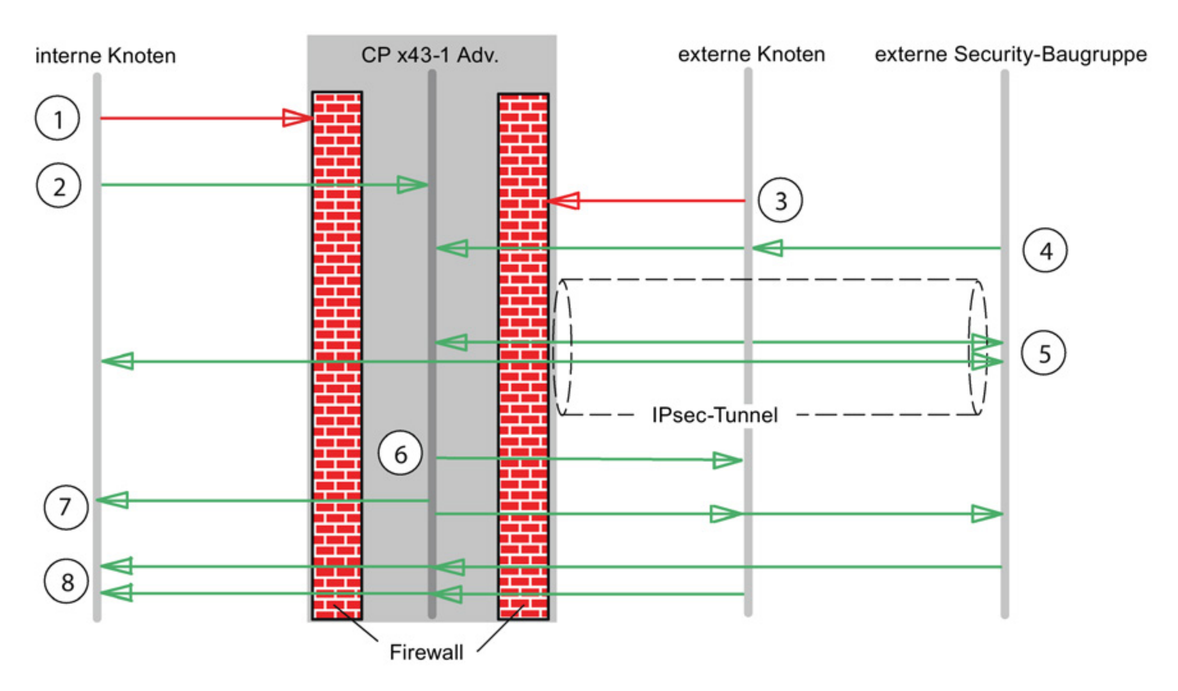


Bild 4-1 Standard-Einstellung für IP-Paketfilter CP x43-1 Adv.

① Alle Telegrammtypen von intern nach extern sind geblockt.

② Alle Telegramme von intern an die Security-Baugruppe sind zugelassen.

③ Alle Telegramme von extern nach intern und an die Security-Baugruppe sind geblockt (auch ICMP-Echo-Request).

④ Telegramme von extern (externe Knoten und externe Security-Baugruppen) an Security-Baugruppe vom folgenden Typ sind zugelassen:

- ESP-Protokoll (Verschlüsselung)
- IKE (Protokoll zum Aufbau der IPsec-Tunnel)
- NAT-Traversal (Protokoll zum Aufbau der IPsec-Tunnel)

⑤ IP-Kommunikation über IPsec-Tunnel ist zugelassen.

⑥ Telegramme vom Typ Syslog sind von der Security-Baugruppe nach extern zugelassen und werden nicht durch die Firewall beeinflusst.

Hinweis

Da Syslog ein ungesichertes Protokoll ist, kann nicht garantiert werden, dass die Log-Daten gesichert übertragen werden.

⑦ Telegramme von der Security-Baugruppe nach intern und extern sind zugelassen.

⑧ Antworten auf Anfragen aus dem internen Netz oder von der Security-Baugruppe sind zugelassen.

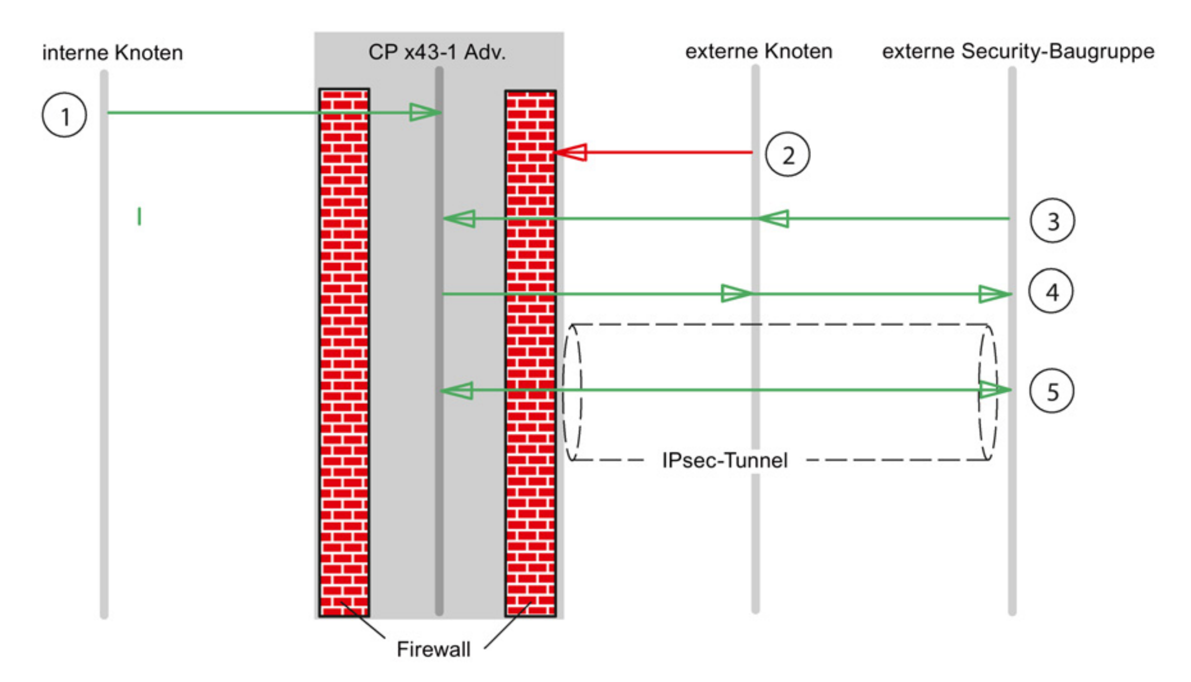


Bild 4-2 Standard-Einstellung für MAC-Paketfilter CP x43-1 Adv.

① Alle Telegramme von intern an die Security-Baugruppe sind zugelassen.

② Alle Telegramme von extern an die Security-Baugruppe sind geblockt.

③ Alle Telegramme von extern an die Security-Baugruppe vom folgenden Typ sind zugelassen:

- ARP mit Bandbreitenbegrenzung
- PROFINET-DCP mit Bandbreitenbegrenzung
- LLDP

④ Telegramme von der Security-Baugruppe nach extern vom folgenden Typ sind zugelassen:

- ARP mit Bandbreitenbegrenzung
- PROFINET-DCP mit Bandbreitenbegrenzung

⑤ Folgende Protokolle, die durch IPsec-Tunnel gesendet werden, sind zugelassen:

- ISO
- LLDP

Hinweis

Keine Kommunikation am VPN-Tunnel vorbei

Zusätzlich wird für alle im Projekt bekannten VPN Partnern verhindert, dass eine Kommunikation zwischen den VPN-Endpunkten am Tunnel vorbei möglich ist. Das Verhalten kann auch nicht durch das Anlegen von entsprechenden Firewall-Regeln im Erweiterten Modus geändert werden.

4.1.1.2 Firewall projektieren

So erreichen Sie diese Funktion

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall".

Tabelle 4- 1 Verfügbare Dienste und Richtungen

Dienst	Station ⇒ Extern Intern ⇒ Extern	Extern ⇒ Intern	Extern ⇒ Station	Extern ⇔ Station	Freigegebe-ne Ports	Bedeutung
Erlaube IP-Kommuni-kation	x	x	x	-	-	Der IP-Verkehr für die ausgewählten Kommu-nikationsrichtungen wird zugelassen.
Erlaube S7-Protokoll	x	x	x	-	TCP Port 102	Kommunikation der Netzwerkteilnehmer über das S7-Protokoll wird zugelassen.
Erlaube FTP/FTPS (expliziter Modus)	x	x	x	-	TCP Port 20 TCP Port 21	Zur Dateiverwaltung und Dateizugriff zwischen Server und Client.
Erlaube HTTP	x	x	x	-	TCP Port 80	Zur Kommunikation mit einem Webserver.
Erlaube HTTPS	x	x	x	-	TCP Port 443	Zur gesicherten Kommunikation mit einem Webserver, z. B. zur Web-Diagnose.
Erlaube DNS	x	x	-	-	TCP Port 53 UDP Port 53	Kommunikationsverbindung zu einem DNS-Server wird zugelassen.
Erlaube SNMP	x	x	x	-	TCP Port 161/162 UDP Port 161/162	Zur Überwachung von SNMP-fähigen Netz-teilnehmern.
Erlaube SMTP	x	x	-	-	TCP Port 25	Zum Austausch von E-Mails zwischen authen-tifizierten Benutzern über einen SMTP-Server.
Erlaube NTP	x	x	-	-	UDP Port 123	Zur Synchronisation der Uhrzeit.

Dienst	Station ⇒ Extern Intern ⇒ Extern	Extern ⇒ Intern	Extern ⇒ Station	Extern ⇔ Station	Freigegebe-ne Ports	Bedeutung
Erlaube MAC-Ebene-Kommuni-kation	-	-	-	x	-	Der MAC-Verkehr von extern zur Station und umgekehrt ist zugelassen.
Erlaube ISO-Kommuni-kation	-	-	-	x	-	Der ISO-Verkehr von extern zur Station und umgekehrt ist zugelassen.

Tabelle 4- 2 Logging für IP- und MAC-Regelsätze

Regelsatz	Aktion bei Aktivierung	Angelegte Regel		
IP-Log-Einstellungen		**Aktion**	**Von**	**Nach**
Aufzeichnen getunnelter Pakete	Nur aktiv, wenn die Security-Baugruppe Teilnehmer einer VPN-Gruppe ist. Alle IP-Pakete, die über den Tunnel weitergeleitet wurden, werden geloggt.	Allow	Station	Tunnel
		Allow	Tunnel	Station
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden IP-Pakete die verworfen wurden, werden geloggt.	Drop	Extern	Station
MAC-Log-Einstellungen		**Aktion**	**Von**	**Nach**
Aufzeichnen blockierter eingehender Pakete zur Station	Alle eintreffenden MAC-Pakete, die verworfen wurden, werden geloggt.	Drop	Extern	Station
Aufzeichnen blockierter ausgehender Pakete von Station	Alle ausgehenden MAC-Pakete, die verworfen wurden, werden geloggt.	Drop	Station	Extern

Hinweis

Datenverkehr über projektierte Verbindungen wird nicht geloggt.

4.1.1.3 Zugriffsliste projektieren

IP-Zugriffsliste / ACL-Einträge ändern

Die Liste erscheint, wenn in STEP 7 im Register IP-Zugriffsschutz das Optionskästchen "IP-Zugriffsschutz für IP-Kommunikation aktivieren" aktiviert ist.

Über die IP-Zugriffslisten stellen Sie den Zugriffsschutz für bestimmte IP-Adressen ein. Bereits in STEP 7 angelegte Listeneinträge mit den entsprechenden Rechten werden in SCT angezeigt.

Das in STEP 7 auswählbare Recht "Ändern der Accessliste (M)" wird nicht nach SCT übertragen. Damit die zusätzliche IP-Zugriffsberechtigungen übermitteln werden kann, müssen Sie dem entsprechenden Benutzer in SCT das Benutzerecht "Web: IP Access Control-Liste erweitern" zuweisen.

Hinweis

Geändertes Verhalten nach Migration

- Nach der Migration wirkt der Zugriffsschutz nur noch an der externen Schnittstelle. Damit der Zugriffsschutz auch an der internen Schnittstelle wirkt, konfigurieren Sie im Erweiterten Modus von SCT die entsprechenden Firewall-Regeln.
- Die Security-Baugruppe antwortet auch auf ARP-Anfragen von nicht freigegebenen IP-Adressen (Layer 2).
- Wenn Sie eine IP Access Control-Liste ohne Einträge migrieren, wird die Firewall aktiviert und auf den CP kann von extern nicht mehr zugegriffen werden. Damit der CP erreichbar ist, konfigurieren Sie in SCT die entsprechenden Firewall-Regeln.

So erreichen Sie diese Funktion

Menübefehl SCT: Markieren Sie die zu bearbeitende Security-Baugruppe und wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften…", Register "Firewall".

Menübefehl STEP 7: "IP-Zugriffsschutz" > "Start der Firewall-Konfiguration", Schaltfläche "Ausführen...".

Tabelle 4- 3 Angaben

Parameter	Bedeutung
IP-Adresse	Zugelassene IP-Adresse oder IP-Adressbereich.
Rechte	Je nach getroffener Zuordnung. Rechte, die für die IP-Adresse freigeschaltet sind.
Kommentar	Zusätzliche Kommentareingabe.
Logging	Aktivieren Sie das Kontrollkästchen, werden die Regeln im Paketfilter-Log aufgezeichnet.
Erweiterten Modus aktivieren	Aktivieren Sie das Kontrollkästchen, werden die Einträge in folgende Firewall-Regeln umgewandelt.

Tabelle 4- 4 Schaltflächen

Bezeichnung	Bedeutung / Auswirkung
Neu...	Legen Sie eine neue IP-Adresse oder einen neuen IP-Adressbereich mit den dazugehörigen Rechten an.
Ändern...	Markieren Sie einen Eintrag und klicken Sie auf diese Schaltfläche, um einen bestehenden Eintrag zu bearbeiten.
Löschen	Löschen Sie über diese Schaltfläche den ausgewählten Eintrag.

4.1.1.4 Eintrag zur Zugriffsliste hinzufügen

Nehmen Sie folgende Einstellungen vor

Feld	Beschreibung
IP-Adresse (oder Start des IP-Bereichs)	Geben Sie die IP-Adresse oder den Anfangswert eines IP-Adressbereichs ein.
Ende des IP-Bereichs (optional)	Geben Sie den Endwert eines IP-Adressbereichs ein.
Kommentar	Zusätzliche Kommentareingabe; beispielsweise zur Beschreibung des Kommunikationspartners oder des Adressbereiches.
Diese IP-Adresse ist für folgende Zugriffe autorisiert	Zugriff auf Station (A=Access): Kommunikationspartner mit Adressen im angegebenen Bereich haben Zugriff auf die dem CP zugehörende Station (CP / CPU). Diese Zugriffsberechtigung ist für IP-Adressen, die Sie in der Verbindungsprojektierung angegeben haben, implizit gesetzt (gilt nur für spezifizierte Verbindungen). IP-Routing zu anderem Subnetz (R=Routing): Kommunikationspartner mit Adressen im angegebenen Bereich haben Zugriff auf weitere am CP angeschlossene Subnetze. Diese Zugriffsberechtigung ist für IP-Adressen, die Sie in der Verbindungsprojektierung angegeben haben, nicht automatisch gesetzt. Bei Bedarf muss dieses Zugriffsrecht hier explizit gesetzt werden.

Weitere Regeln zur Eingabe:

- Es wird geprüft, ob Einzeladressen mehrfach enthalten sind; hierbei werden erkannt: mehrfache Einzelangabe; Bereichsüberschneidungen.
- Einzeln angegebene IP-Adressen können auch zusätzlich innerhalb eines Bereiches vorkommen; es gelten dann die insgesamt einer IP-Adresse zugewiesenen Zugriffsberechtigungen.
- Es wird nicht geprüft, ob in einem Bereich ungültige Adressen enthalten sind (z. B. können Subnetz-Broadcast-Adressen hier angegeben werden, obwohl sie nicht als IP-Adresse eines Absenders auftreten können).

4.1.2 CP 1628

4.1.2.1 Voreinstellung der Firewall

Verhalten mit Voreinstellung

Die folgenden Diagramme zeigen die Standard-Einstellungen im Detail jeweils für den IP-Paketfilter und den MAC-Paketfilter, wenn das Kontrollkästchen "Firewall aktivieren" aktiviert ist und auch im Erweiterten Modus keine Regeln vorhanden sind. Das Verhalten kann durch das Anlegen von entsprechenden Firewall-Regeln im Erweiterten Modus geändert werden.

Standard-Einstellung für CP 1628

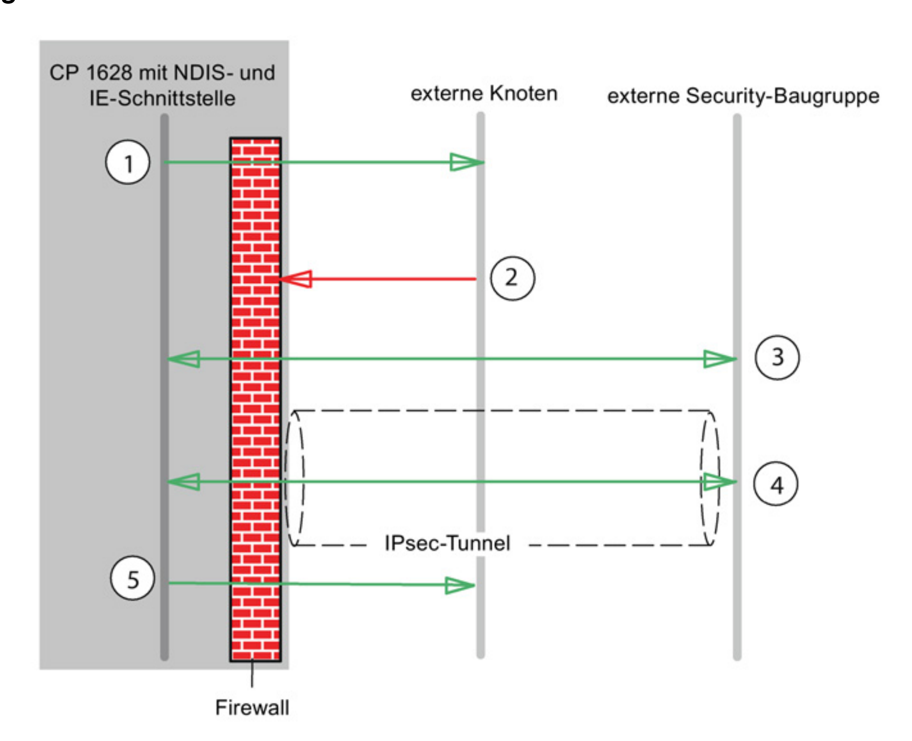


Bild 4-3 Standard-Einstellung für IP-Paketfilter CP 1628

① Alle Telegramme von NDIS- und IE (Industrial Ethernet)-Schnittstelle nach extern sind zugelassen.

② Alle Telegramme von extern sind geblockt.

③ Alle Telegramme von extern an die Security-Baugruppe und umgekehrt vom folgenden Typ sind zugelassen:

- ESP-Protokoll (Verschlüsselung)
- IKE (Protokoll zum Aufbau der IPsec-Tunnel)
- NAT-Traversal (Protokoll zum Aufbau der IPsec-Tunnel)

④ IP-Kommunikation über IPsec-Tunnel ist zugelassen.

⑤ Telegramme vom Typ Syslog sind von der Security-Baugruppe nach extern zugelassen.

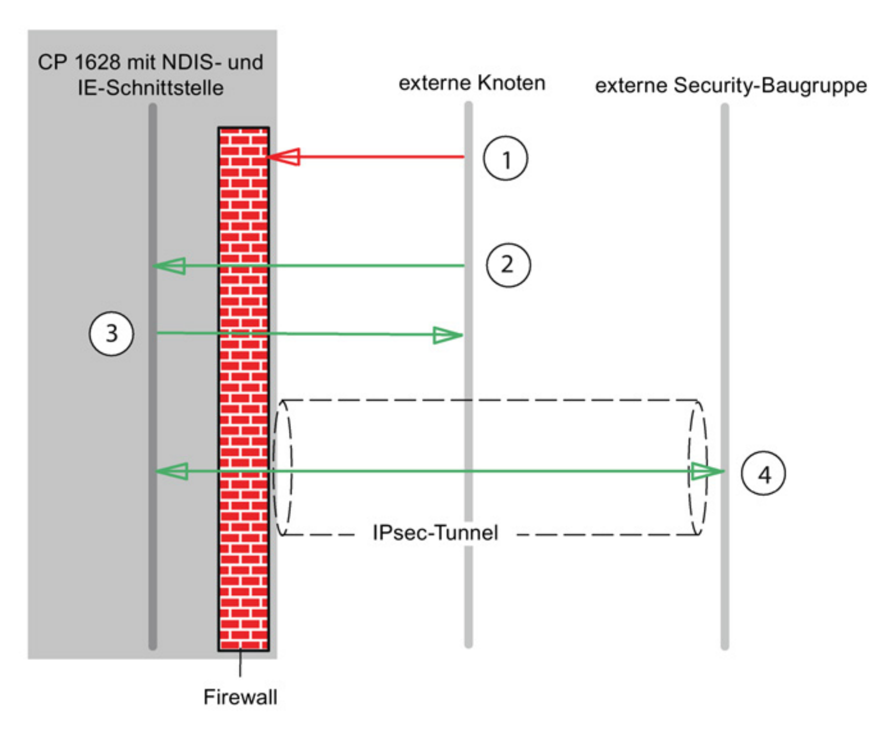


Bild 4-4 Standard-Einstellung für MAC-Paketfilter CP 1628

① Alle Telegramme von extern sind geblockt.

② Alle Telegramme von extern vom folgenden Typ sind zugelassen:

- ARP mit Bandbreitenbegrenzung
- PROFINET-DCP mit Bandbreitenbegrenzung

③ Telegramme von der Security-Baugruppe nach extern vom folgenden Typ sind zugelassen:

- PROFINET-DCP mit Bandbreitenbegrenzung

④ MAC-Protokolle, die durch IPsec-Tunnel gesendet werden, sind zugelassen.

Hinweis

Keine Kommunikation am VPN-Tunnel vorbei

Zusätzlich wird für alle im Projekt bekannten VPN Partnern verhindert, dass eine Kommunikation zwischen den VPN-Endpunkten am Tunnel vorbei möglich ist. Das Verhalten kann auch nicht durch das Anlegen von entsprechenden Firewall-Regeln im Erweiterten Modus geändert werden.

4.1.2.2 Firewall projektieren

So erreichen Sie diese Funktion

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall".

Tabelle 4- 5 Verfügbare Dienste und Richtungen

Dienst	Extern ⇒ Station	Extern ⇔ Station	Freigegebene Ports	Bedeutung
Erlaube IP-Kommunikation	x	-	-	Der IP-Verkehr für die ausgewählten Kommunikationsrichtungen wird zugelassen.
Erlaube S7-Protokoll	x	-	TCP Port 102	Kommunikation der Netzwerkteilnehmer über das S7-Protokoll wird zugelassen.
Erlaube FTP/FTPS (expliziter Modus)	x	-	TCP Port 20 TCP Port 21	Zur Dateiverwaltung und Dateizugriff zwischen Server und Client.
Erlaube HTTP	x	-	TCP Port 80	Zur Kommunikation mit einem Webserver.
Erlaube HTTPS	x	-	TCP Port 443	Zur gesicherten Kommunikation mit einem Webserver, z. B. zur Web-Diagnose.
Erlaube DNS	x	-	TCP Port 53 UDP Port 53	Kommunikationsverbindung zu einem DNS-Server wird zugelassen.
Erlaube SNMP	x	-	TCP Port 161/162 UDP Port 161/162	Zur Überwachung von SNMP-fähigen Netzteilnehmern.
Erlaube SMTP	x	-	TCP Port 25	Zum Austausch von E-Mails zwischen authentifizierten Benutzern über einen SMTP-Server.
Erlaube NTP	x	-	UDP Port 123	Zur Synchronisation der Uhrzeit.
Erlaube MAC-Ebene-Kommunikation	-	x	-	Der MAC-Verkehr von extern zur Station und umgekehrt ist zugelassen.
Erlaube ISO-Kommunikation	-	x	-	Der ISO-Verkehr von extern zur Station und umgekehrt ist zugelassen.
Erlaube SiCLOCK	-	x	-	SiCLOCK-Uhrzeittelegramme von extern zur Station und umgekehrt sind zugelassen.

Tabelle 4- 6 Logging für IP- und MAC-Regelsätze

Regelsatz	**Aktion bei Aktivierung**	**Angelegte Regel**		
IP-Log-Einstellungen		**Aktion**	**Von**	**Nach**
Aufzeichnen getunnelter Pakete	Nur aktiv, wenn die Security-Baugruppe Teilnehmer einer VPN-Gruppe ist. Alle IP-Pakete, die über den Tunnel weitergeleitet wurden, werden geloggt.	Allow	Station	Tunnel
		Allow	Tunnel	Station
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden IP-Pakete, die verworfen wurden, werden geloggt.	Drop	Extern	Station
MAC-Log-Einstellungen		**Aktion**	**Von**	**Nach**
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden MAC-Pakete, die verworfen wurden, werden geloggt.	Drop	Extern	Station
Aufzeichnen blockierter ausgehender Pakete	Alle ausgehenden MAC-Pakete, die verworfen wurden, werden geloggt.	Drop	Station	Extern

Hinweis

Datenverkehr über projektierte Verbindungen wird nicht geloggt.

4.2 SCALANCE S im Standard Modus

4.2.1 Voreinstellung der Firewall

Verhalten mit Voreinstellung

Die folgenden Diagramme zeigen die Standardeinstellungen im Detail jeweils für den IP-Paketfilter und den MAC-Paketfilter. Das Verhalten kann durch das Anlegen von entsprechenden Firewall-Regeln im Erweiterten Modus geändert werden.

Standardeinstellung für SCALANCE S602/S612 ab V3

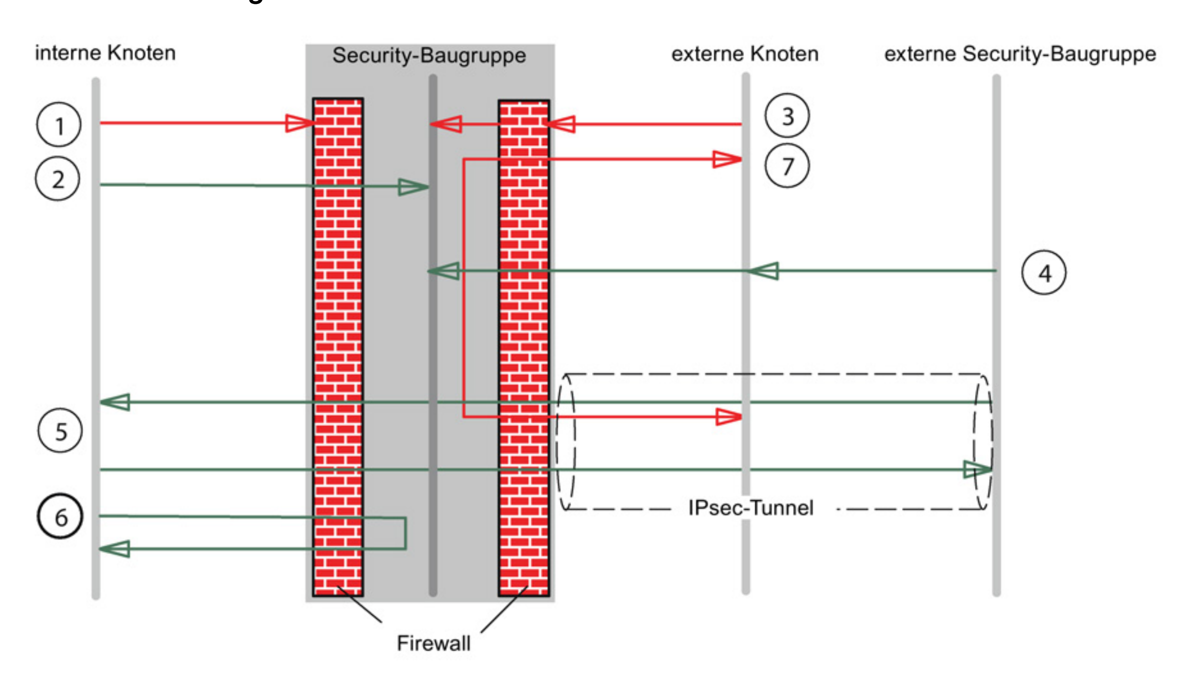


Bild 4-5 Standardeinstellung für IP-Paketfilter SCALANCE S602/S612 ab V3

① Alle Telegrammtypen von intern nach extern sind geblockt.

② Alle Telegramme von intern an die Security-Baugruppe sind zugelassen.

③ Alle Telegramme von extern nach intern und an die Security-Baugruppe sind geblockt.

④ Telegramme von extern (externe Knoten und externe Security-Baugruppen) an die Security-Baugruppe sind vom folgenden Typ sind zugelassen:

- HTTPS (SSL)
- ESP-Protokoll (Verschlüsselung)
- IKE (Protokoll zum Aufbau der IPsec-Tunnel)
- NAT-Traversal (Protokoll zum Aufbau der IPsec-Tunnel)

⑤ IP-Kommunikation über IPsec-Tunnel ist zugelassen. S602

⑥ Telegramme von intern nach intern sind zugelassen.

⑦ Telegramme von extern auf Tunnel an der externen Schnittstelle und umgekehrt sind geblockt. S602

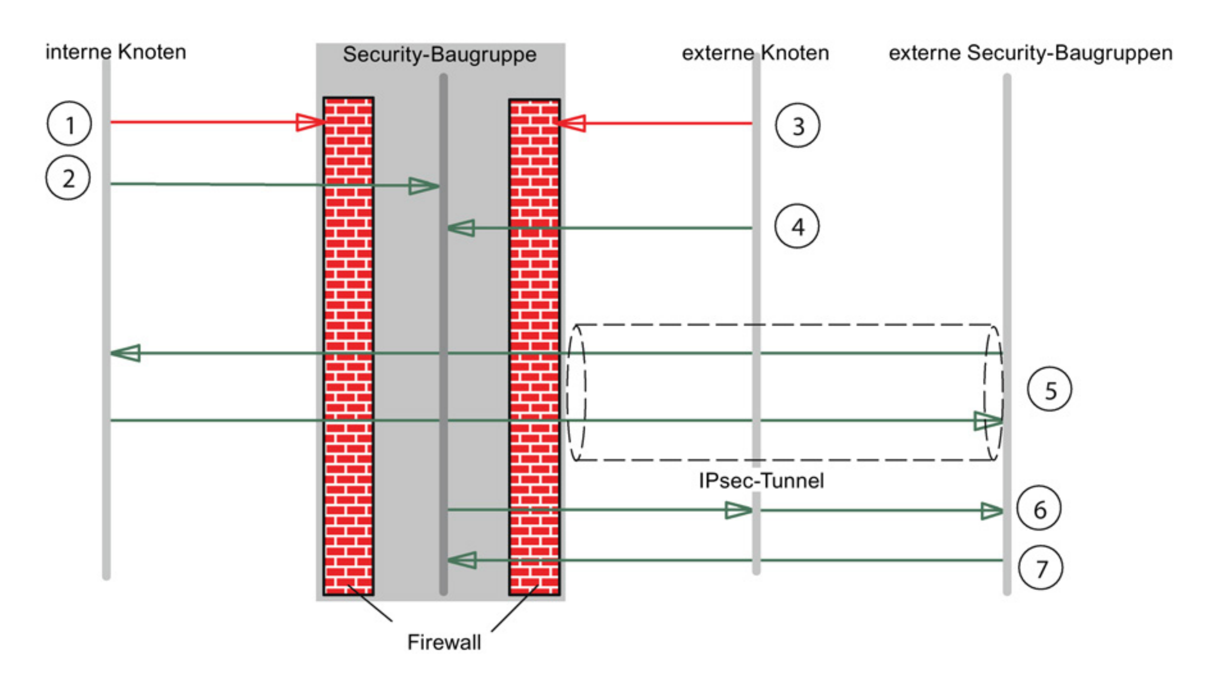


Bild 4-6 Standardeinstellung für MAC- Paketfilter SCALANCE S602/612 ab V3

① Alle Telegrammtypen von intern nach extern außer den folgenden Telegrammtypen sind geblockt.

- ARP-Telegramme

② Alle Telegramme von intern an die Security-Baugruppe sind zugelassen.

③ Alle Telegramme von extern nach intern außer den folgenden Telegrammtypen sind geblockt.

- ARP-Telegramme mit Bandbreitenbegrenzung

④ Telegramme von extern an die Security-Baugruppe vom folgenden Typ sind zugelassen:

- ARP mit Bandbreitenbegrenzung
- PROFINET-DCP mit Bandbreitenbegrenzung
- Im Routing-Modus: LLDP-Telegramme (Ethertype 0x88CC) S≥V4.0

⑤ Im Bridge-Modus: MAC-Protokolle, die durch IPsec-Tunnel gesendet werden, sind zugelassen.

⑥ Telegramme von der Security-Baugruppe nach extern vom folgenden Typ sind zugelassen:

- PROFINET
- Im Routing-Modus: LLDP-Telegramme (Ethertype 0x88CC) S≥V4.0

⑦ Multicast- und Broadcast-Telegramme von extern an die Security-Baugruppe vom folgenden Typ sind zugelassen:

- PROFINET mit Bandbreitenbegrenzung

Hinweis

Automatische Freischaltung von Ethertypes

Wenn PPPoE aktiv ist, werden die Ethertypes 0x8863 und 0x8864 automatisch freigeschaltet (PPPoE Discovery und Session Stage).

Standardeinstellung für SCALANCE S623 ab V3 und S627-2M V4

Die standardmäßigen Firewall-Regeln für die externe und interne Schnittstelle entsprechen denen, die für SCALANCE S-Baugruppen vom Typ S602 und S612 gelten. In den folgenden beiden Grafiken sind lediglich diejenigen IP-Paketfilter-Regeln dargestellt, die die DMZ-Schnittstelle betreffen. MAC-Paketfilter-Regeln können für die DMZ-Schnittstelle nicht definiert werden, weil die Telegramme hierbei zwischen externem bzw. internem Netz und DMZ-Schnittstelle geroutet werden.

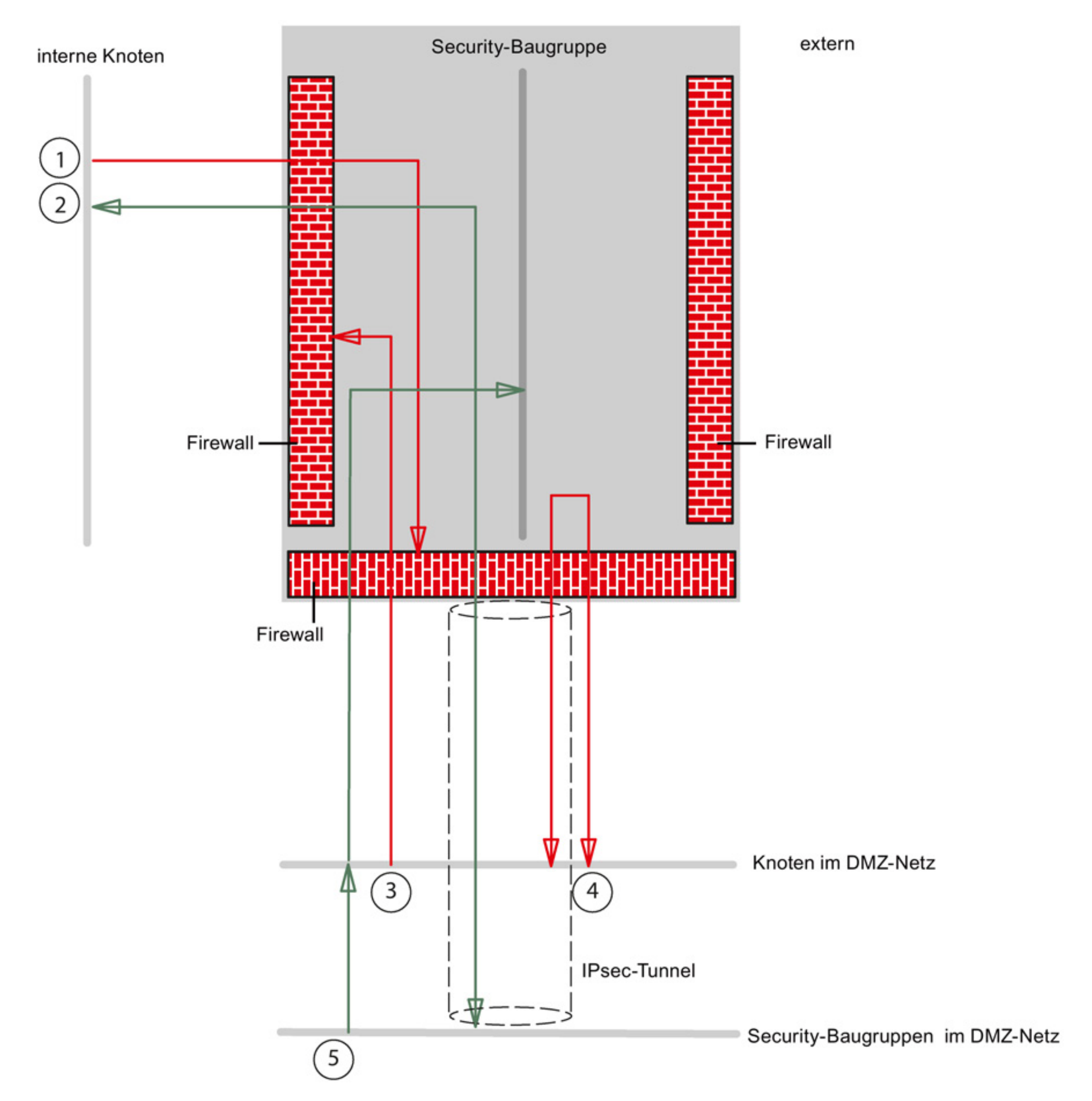


Bild 4-7 Standardeinstellung für IP-Paketfilter SCALANCE S623/S627-2M (Verkehr zwischen DMZ-Netz und internem Netz bzw. DMZ-Netz und Security-Baugruppe)

① Alle Telegramme von intern ins DMZ-Netz sind geblockt.

② Alle Telegramme von intern nach Tunnel auf DMZ-Schnittstelle und umgekehrt sind zugelassen.

③ Alle Telegramme vom DMZ-Netz nach intern sind geblockt.

④ Alle Telegramme vom DMZ-Netz nach Tunnel auf DMZ-Schnittstelle und umgekehrt sind geblockt.

⑤ Telegramme vom DMZ-Netz (Knoten im DMZ-Netz und Security-Baugruppen im DMZ-Netz) an die Security-Baugruppe sind vom folgenden Typ zugelassen:

- HTTPS (SSL)
- ESP-Protokoll (Verschlüsselung)
- IKE (Protokoll zum Aufbau der IPSec-Tunnel)
- NAT-Traversal (Protokoll zum Aufbau der IPsec-Tunnel)

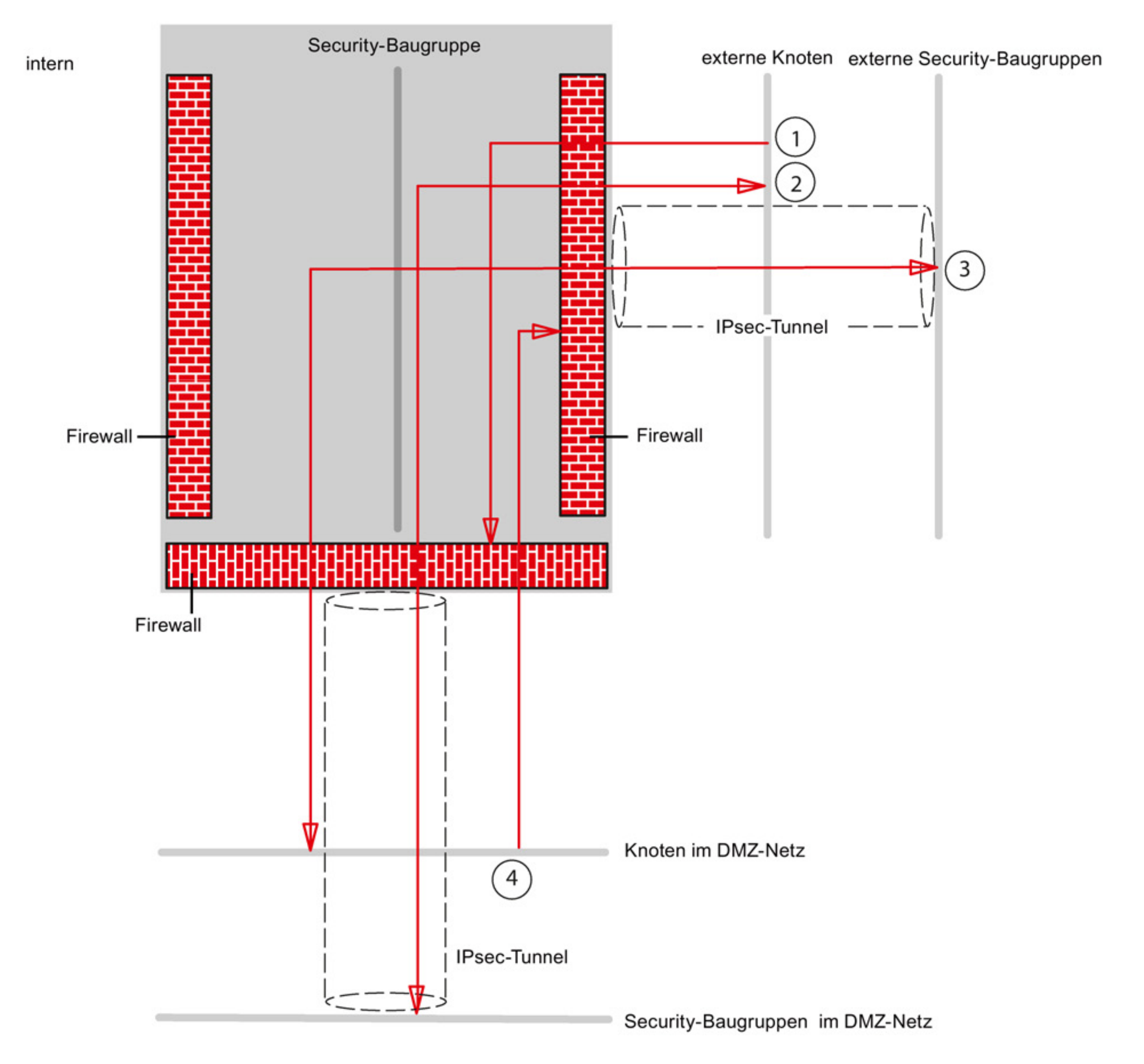


Bild 4-8 Standardeinstellung für IP-Paketfilter SCALANCE S623/S627-2M (Verkehr zwischen DMZ-Netz und externem Netz)

① Alle Telegramme von extern ins DMZ-Netz sind geblockt.

② Alle Telegramme von extern nach Tunnel auf DMZ-Schnittstelle und umgekehrt sind geblockt.

③ Alle Telegramme vom DMZ-Netz nach Tunnel auf externer Schnittstelle und umgekehrt sind geblockt.

④ Alle Telegramme vom DMZ-Netz nach extern sind geblockt

Hinweis

Automatische Freischaltung von Ethertypes

Wenn PPPoE aktiv ist, werden die Ethertypes 0x8863 und 0x8864 automatisch freigeschaltet (PPPoE Discovery und Session Stage).

4.2.2 Firewall projektieren für SCALANCE S ≥ V3.0

So erreichen Sie diese Funktion

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall".

Firewall standardmäßig aktiviert

Das Kontrollkästchen "Firewall aktivieren" ist standardmäßig aktiviert. Die Firewall ist also automatisch aktiv und alle Zugriffe von extern auf die Security-Baugruppe sind gesperrt. Im Standard Modus schalten Sie durch Anklicken der entsprechenden Kontrollkästchen die Firewall für die jeweiligen Richtungen frei.

Detaillierte Firewall-Einstellungen im Erweiterten Modus

Im Erweiterten Modus können Sie Firewall-Regeln auf einzelne Teilnehmer beschränken, siehe folgendes Kapitel:

- Firewall im Erweiterten Modus (Seite 139)

Firewall-Projektierung mit VPN

Befindet sich die Security-Baugruppe in einer VPN-Gruppe und ist im Standard Modus das Kontrollkästchen "Ausschließlich getunnelte Kommunikation" aktiviert, so ist über die externe Schnittstelle oder über die DMZ-Schnittstelle nur verschlüsselter IPsec-Datentransfer zugelassen. Lediglich der HTTPS-Zugriff auf das Modul (TCP-Port 443) ist weiterhin ungetunnelt zugelassen.

Deaktivieren Sie das Kontrollkästchen, dann sind die getunnelte Kommunikation und zusätzlich die in den anderen Auswahlboxen angewählten Kommunikationsarten zugelassen.

Tabelle 4- 7 Verfügbare Firewall-Regeln und Richtungen (IP-Verkehr)

Dienst	Intern ⇒ Extern	Extern ⇒ Intern	Intern => DMZ S62x	DMZ => Intern S62x	Von Intern	Von Extern	Freigegebene Ports	Bedeutung
Erlaube IP-Kommunikation	x	x	x	x	-	-	-	IP-Kommunikation für die ausgewählten Kommunikationsrichtungen wird zugelassen.
Erlaube S7-Protokoll	x	x	x	x	-	-	TCP Port 102	Kommunikation der Netzwerkteilnehmer über das S7-Protokoll wird zugelassen.
Erlaube FTP/FTPS (expliziter Modus)	x	x	x	x	-	-	TCP Port 20 TCP Port 21	Zur Dateiverwaltung und Dateizugriff zwischen Server und Client.
Erlaube HTTP	x	x	x	x	-	-	TCP Port 80	Zur Kommunikation mit einem Webserver.
Erlaube HTTPS	x	x	x	x	-	-	TCP Port 443	Zur gesicherten Kommunikation mit einem Webserver, z. B. zur Web-Diagnose.
Erlaube DNS	x	x	x	x	-	-	TCP Port 53 UDP Port 53	Kommunikationsverbindung zu einem DNS-Server wird zugelassen.
Erlaube SNMP	x	x	x	x	-	-	TCP Port 161/162 UDP Port 161/162	Zur Überwachung von SNMP-fähigen Netzteilnehmern.
Erlaube SMTP	x	x	x	x	-	-	TCP Port 25	Zum Austausch von E-Mails zwischen authentifizierten Benutzern über einen SMTP-Server.
Erlaube NTP	x	x	x	x	-	-	UDP Port 123	Zur Synchronisation der Uhrzeit.
Erlaube DHCP	x	x	x	x	-	-	UDP Port 67 UDP Port 68	Kommunikation mit einem DHCP-Server wird zugelassen.

Dienst	Intern ⇒ Extern	Extern ⇒ Intern	Intern => DMZ S62x	DMZ => Intern S62x	Von Intern	Von Extern	Freigegebene Ports	Bedeutung
Erlaube MAC-Ebene-Kommunikation	-	-	-	-	x	x	-	Der MAC-Verkehr von intern nach extern und umgekehrt ist zugelassen.
Erlaube ISO-Kommunikation	-	-	-	-	x	x	-	Der ISO-Verkehr von intern nach extern und umgekehrt ist zugelassen.
Erlaube SiCLOCK	-	-	-	-	x	x	-	SiClock-Uhrzeittelegramme von intern nach extern und umgekehrt sind zugelassen.
Erlaube DCP	-	-	-	-	x	x	-	DCP-Verkehr zur Vergabe von IP-Adressen ist von intern nach extern und umgekehrt zugelassen.

Tabelle 4- 8 Logging für IP- und MAC-Regelsätze

Regelsatz	Aktion bei Aktivierung
IP-Log-Einstellungen	
Aufzeichnen getunnelter Pakete	Nur aktiv, wenn die Security-Baugruppe Teilnehmer einer VPN-Gruppe ist. Alle IP-Pakete, die über den Tunnel weitergeleitet wurden, werden geloggt.
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden IP-Pakete, die verworfen wurden, werden geloggt.
Aufzeichnen blockierter ausgehender Pakete	Alle ausgehenden IP-Pakete, die verworfen wurden, werden geloggt.
MAC-Log-Einstellungen	
Aufzeichnen getunnelter Pakete	Nur aktiv, wenn die Security-Baugruppe Teilnehmer einer VPN-Gruppe ist. Alle MAC-Pakete, die über den Tunnel weitergeleitet wurden, werden geloggt.
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden MAC-Pakete, die verworfen wurden, werden geloggt.
Aufzeichnen blockierter ausgehender Pakete	Alle ausgehenden MAC-Pakete, die verworfen wurden, werden geloggt.

4.2.3 Firewall projektieren für SCALANCE S < V3.0

So erreichen Sie diese Funktion

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall".

Hinweis

Detaillierte Firewall-Einstellungen im Erweiterten Modus

Im Erweiterten Modus können Sie Firewall-Regeln auf einzelne Teilnehmer beschränken.

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sie können eine einmal vorgenommene Umschaltung in den Erweiterten Modus für das aktuelle Projekt nicht mehr rückgängig machen.

Abhilfe für SCT Standalone: Schließen Sie das Projekt ohne zu speichern und öffnen Sie es erneut.

Tabelle 4- 9 Verfügbare Dienste und Richtungen

Regel / Option	Freigegebene Ports	Funktion
Ausschließlich getunnelte Kommunikation	-	Das ist die Standardeinstellung. Die Option ist nur dann wählbar, wenn sich die Security-Baugruppe in einer VPN-Gruppe befindet. Mit dieser Einstellung wird nur verschlüsselter IPsec-Datentransfer zugelassen; nur Knoten, welche durch Security-Baugruppen mit VPN-Mechanismen geschützt werden, können miteinander kommunizieren. Wenn diese Option abgewählt ist, dann ist die getunnelte Kommunikation und zusätzlich die in den anderen Auswahlboxen angewählte Kommunikationsart zugelassen.
Erlaube IP-Kommunikation vom internen ins externe Netz	-	Interne Knoten können eine Kommunikationsverbindung zu Knoten im externen Netz initiieren. Nur Antworttelegramme aus dem externen Netz werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.
Erlaube IP-Kommunikation mit S7-Protokoll vom internen ins externe Netz	TCP Port 102	Interne Knoten können eine S7-Kommunikationsverbindung zu Knoten im externen Netz initiieren. Nur Antworttelegramme aus dem externen Netz werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.
Erlaube Zugriff auf DHCP-Server vom internen ins externe Netz	UDP Port 67 UDP Port 68	Interne Knoten können eine Kommunikationsverbindung zu einem DHCP-Server im externen Netz initiieren. Nur die Antworttelegramme des DHCP-Servers werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.

Regel / Option	Freigegebene Ports	Funktion
Erlaube Zugriff auf NTP-Server vom internen ins externe Netz	UDP Port 123	Interne Knoten können eine Kommunikationsverbindung zu einem NTP-Server (Network Time Protocol) im externen Netz initiieren. Nur die Antworttelegramme des NTP-Servers werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.
Erlaube SiClock-Uhrzeittelegramme vom externen ins interne Netz	-	Mit dieser Option werden SiClock-Uhrzeittelegramme vom externen ins interne Netz freigegeben.
Erlaube Zugriff auf DNS-Server vom internen ins externe Netz	TCP Port 53 UDP Port 53	Interne Knoten können eine Kommunikationsverbindung zu einem DNS-Server im externen Netz initiieren. Nur die Antworttelegramme des DNS-Servers werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.
Erlaube die Konfiguration von Netzknoten mittels DCP	-	Das DCP-Protokoll wird vom PST-Tool verwendet, um bei SIMATIC NET Netzkomponenten die Knotentaufe (Einstellen der IP-Parameter) vorzunehmen. Mit dieser Regel wird Knoten im externen Netz erlaubt, per DCP-Protokoll auf Knoten im internen Netz zuzugreifen.

Tabelle 4- 10 Logging für IP- und MAC-Regelsätze

Regelsatz	Aktion bei Aktivierung
IP-Log-Einstellungen	
Aufzeichnen getunnelter Pakete	Nur wenn die Security-Baugruppe Teilnehmer einer VPN-Gruppe ist: Alle IP-Pakete, die über den Tunnel weitergeleitet wurden, werden geloggt.
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden IP-Pakete, die verworfen wurden, werden geloggt.
Aufzeichnen blockierter ausgehender Pakete	Alle ausgehenden IP-Pakete, die verworfen wurden, werden geloggt.
MAC-Log-Einstellungen	
Aufzeichnen getunnelter Pakete	Nur wenn die Security-Baugruppe Teilnehmer einer VPN-Gruppe ist: Alle MAC-Pakete, die über den Tunnel weitergeleitet wurden, werden geloggt.
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden MAC-Pakete, die verworfen wurden, werden geloggt.
Aufzeichnen blockierter ausgehender Pakete	Alle ausgehenden MAC-Pakete, die verworfen wurden, werden geloggt.

4.3 Firewall im Erweiterten Modus

Im Erweiterten Modus gibt es erweiterte Einstellmöglichkeiten, die eine individuelle Einstellung der Firewall-Regeln und der Sicherheitsfunktionalität zulassen.

In den Erweiterten Modus umschalten

Schalten Sie für alle in diesem Kapitel beschriebenen Funktionen in den Erweiterten Modus um.

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.

Abhilfe SCT Standalone: Schließen Sie das Projekt ohne zu speichern und öffnen Sie es erneut.

Symbolische Namen werden unterstützt

Sie können in den nachfolgend beschriebenen Funktionen IP-Adressen oder MAC-Adressen auch als symbolische Namen eingeben. Für weitere Informationen zu symbolischen Namen, siehe Kapitel:

- Symbolische Namen für IP-/MAC-Adressen vergeben (Seite 64)

4.3.1 Firewall im Erweiterten Modus projektieren

Bedeutung

Im Gegensatz zur Projektierung fest vorgegebener Paketfilter-Regeln im Standard Modus können Sie im Erweiterten Modus von Security Configuration Tool individuelle Paketfilter-Regeln projektieren.

Die Paketfilter-Regeln stellen Sie in wählbaren Registern für folgende Protokolle ein:

- Layer 3, 4: IP-Protokoll, IP-Dienste
- Layer 2: MAC-Protokoll, MAC-Dienste

Hinweis

Keine MAC-Regeln bei aktiviertem Routing-Modus



Wenn Sie für die Security-Baugruppe den Routing-Modus aktiviert haben, finden MAC-Regeln keine Anwendung (Dialoge sind inaktiv).

Wenn Sie in den nachfolgend beschriebenen Dialogen keine Regel eintragen, gelten die Standardeinstellungen der Firewall. Details hierzu finden Sie in folgendem Kapitel:

- Standardeinstellungen von CP x43-1 Adv.: Voreinstellung der Firewall (Seite 118)
- Standardeinstellungen von CP 1628: Voreinstellung der Firewall (Seite 124)
- Standardeinstellungen von SCALANCE S: Voreinstellung der Firewall (Seite 128)

Globale, benutzerspezifische und lokale Definition möglich

- Globale Firewall-Regelsätze können mehreren Security-Baugruppen gleichzeitig zugewiesen werden. Sie werden im Erweiterten Modus im Navigationsbereich des Security Configuration Tools angezeigt und global projektiert.
- Benutzerspezifische IP-Regelsätze können einzelnen oder mehreren Security-Baugruppen gleichzeitig zugewiesen werden. Sie werden im Erweiterten Modus im Navigationsbereich des Security Configuration Tools angezeigt und global projektiert. SCALANCE S V4 (RADIUS): Benutzerspezifischen IP-Regelsätzen können neben einzelnen oder mehreren Benutzern auch einzelne oder mehrere Rollen zugewiesen sein.
- Lokale Firewall-Regeln sind jeweils einer Security-Baugruppe zugewiesen. Sie werden im Eigenschaftsdialog der Security-Baugruppen projektiert.

Einer Security-Baugruppe können mehrere lokale Firewall-Regeln, mehrere globale Firewall-Regelsätze und mehrere benutzerspezifische IP-Regelsätze zugewiesen werden.

4.3.2 Globale Firewall-Regelsätze

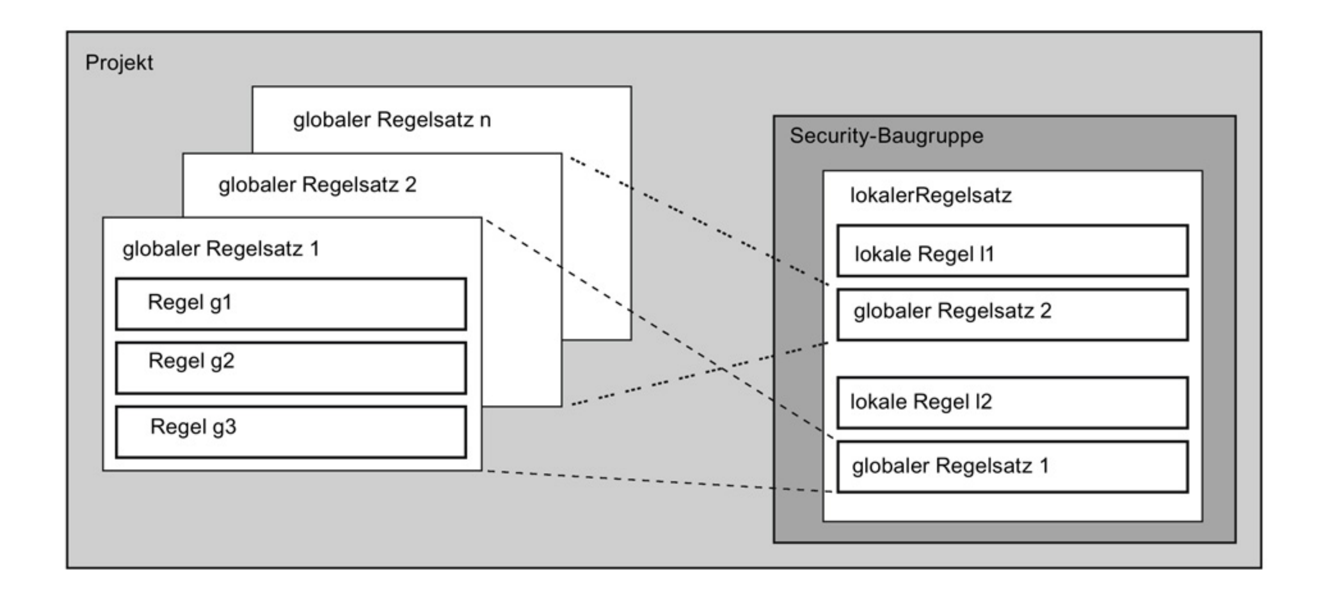
Anwendung

Globale Firewall-Regelsätze werden baugruppenunabhängig auf Projektebene projektiert und sind im Navigationsbereich des Security Configuration Tools sichtbar. Ein globaler Firewall-Regelsatz besteht aus einer oder mehreren Firewall-Regeln und wird mehreren Security-Baugruppen zugewiesen.

Unterschieden wird bei den globalen Firewall-Regelsätzen zwischen:

- IP-Regelsätzen
- MAC-Regelsätzen

Die folgende Darstellung verdeutlicht den Zusammenhang zwischen global definierten Regelsätzen und lokal verwendeten Regelsätzen.



Wann sind globale Firewall-Regelsätze sinnvoll?

Globale Firewall-Regelsätze sind dann sinnvoll, wenn Sie für mehrere Security-Baugruppen identische Filterkriterien für die Kommunikation definieren wollen.

Hinweis

Nur Firewall-Regelsätze zuweisen, die von der Security-Baugruppe unterstützt werden

Eine fehlerhafte Zuordnung von Firewall-Regelsätzen kann zu unerwünschten Ergebnissen führen. Überprüfen Sie daher immer die baugruppenspezifischen lokalen Firewall-Regeln im Ergebnis. Eine falsche Zuordnung wird bei der automatischen Konsistenzprüfung nicht erkannt. Es werden nur die Regeln übernommen, die die Security-Baugruppe auch unterstützt.

Siehe auch

Benutzerspezifische IP-Regelsätze (Seite 143)

4.3.2.1 Globale Firewall-Regelsätze - Vereinbarungen

Globale Firewall-Regelsätze werden lokal genutzt

Folgende Vereinbarungen gelten bei der Erstellung eines globalen Firewall-Regelsatzes sowie bei der Zuweisung zu einer Security-Baugruppe:

- Projektierungsansicht

  Globale Firewall-Regelsätze können nur im Erweiterten Modus angelegt werden.
- Priorität

  Lokal definierte Firewall-Regeln haben standardmäßig eine höhere Priorität als globale Firewall-Regelsätze, die lokal zugewiesen wurden. Globale Firewall-Regelsätze werden daher in der lokalen Regelliste zunächst unten eingefügt.

  Die Priorität kann durch Verändern der Platzierung in der Regelliste verändert werden.
- Regelsätze eingeben, ändern oder löschen

  Globale Firewall-Regelsätze sind in der lokalen Regelliste der Firewall-Regeln bei den Baugruppeneigenschaften nicht editierbar. Sie können dort nur angezeigt und gemäß der gewünschten Priorität platziert werden.

  In der lokalen Regelliste kann eine einzelne Firewall-Regel eines zugeordneten globalen Firewall-Regelsatzes nicht gelöscht werden. Es kann nur der komplette Firewall-Regelsatz aus der lokalen Regelliste entfernt werden. Eine Anpassung des globalen Regelsatzes ist über den Eigenschaftsdialog des globalen Regelsatzes jederzeit möglich. Alle betroffenen Geräte dieser Änderung müssen danach neu geladen werden.

4.3.2.2 Globale Firewall-Regelsätze anlegen und zuweisen

So erreichen Sie diese Funktion

1. Wählen Sie im Navigationsbereich einen der folgenden Ordner:
   - "Globale Firewall-Regelsätze" > "Firewall IP-Regelsätze"
   - "Globale Firewall-Regelsätze" > "Firewall MAC-Regelsätze"
2. Wählen Sie den Menübefehl "Einfügen" > "Firewall-Regelsatz".
3. Geben Sie die folgenden Daten ein:
   - Name: Projektweit eindeutige Bezeichnung des Regelsatzes. Der Name erscheint nach der Zuweisung des Regelsatzes in der lokalen Regelliste der Security-Baugruppe.
   - Beschreibung: Geben Sie eine Beschreibung für den globalen Regelsatz ein.
4. Klicken Sie auf die Schaltfläche "Regel hinzufügen".

5. Tragen Sie der Reihe nach die Firewall-Regeln in die Liste ein. Beachten Sie die Parameterbeschreibung in folgenden Kapiteln:

   Für IP-Regelsätze: IP-Paketfilter-Regeln (Seite 151).

   Für MAC-Regelsätze: MAC-Paketfilter-Regeln (Seite 161).

6. Ordnen Sie den globalen Firewall-Regelsatz den Security-Baugruppen zu, in denen dieser verwendet werden soll. Markieren Sie dazu im Navigationsbereich den globalen Firewall-Regelsatz und ziehen Sie diesen auf die Security-Baugruppen im Navigationsbereich (Drag and Drop). Alternativ können Sie die Zuordnung in der lokalen Regelliste einer Security-Baugruppe über die Schaltfläche "Regelsätze hinzufügen..." vornehmen.

Ergebnis

Der globale Firewall-Regelsatz wird von den Security-Baugruppen als lokaler Regelsatz verwendet und erscheint automatisch in deren baugruppenspezifischen Listen der Firewall-Regeln.

Siehe auch

Globale Firewall-Regelsätze - Vereinbarungen (Seite 142)

4.3.3 Benutzerspezifische IP-Regelsätze



Bedeutung

Benutzerspezifischen IP-Regelsätzen werden zunächst einzelne oder mehrere Benutzer zugewiesen. Anschließend werden die benutzerspezifischen IP-Regelsätze einzelnen oder mehreren Security-Baugruppen zugeordnet. Dadurch ist es möglich, benutzerspezifische Zugriffe zu erlauben. Wenn z. B. standardmäßig alle Zugriffe auf die Netze hinter einer Security-Baugruppe gesperrt sind, können bestimmte Teilnehmer über ihre IP-Adressen für einen Benutzer temporär freigeschaltet werden. Somit ist für diesen Benutzer der Zugriff erlaubt, für andere Benutzer bleiben die Zugriffe weiterhin gesperrt. Die Antworten auf benutzerspezifische Zugriffe werden stets automatisch zugelassen. Es müssen also lediglich IP-Regeln für die initiative Richtung projektiert werden.

Anmelden des Benutzers über das Internet

Der Benutzer kann sich über die Webseite der Security-Baugruppe an der externen Schnittstelle oder an der DMZ-Schnittstelle anmelden. Wenn die Authentifizierung erfolgreich ist, wird der für den Benutzer definierte IP-Regelsatz für die IP-Adresse des Geräts, von dem die Anmeldung erfolgt ist, aktiviert.

Die Verbindung zur Webseite der Security-Baugruppe erfolgt über HTTPS unter Verwendung der IP-Adresse des angebundenen Ports bei Beachtung der gültigen Routing-Regeln:

Beispiel:

Externe Schnittstelle: 192.168.10.1

Aufruf der Login-Seite über: https://192.168.10.1/

Anmelden können sich Benutzer mit jeder Rolle, sofern der Benutzer oder die Rolle einem benutzerspezifischen IP-Regelsatz zugeordnet ist.

Möglichkeiten zur Authentifizierung des Benutzers

Je nachdem, welche Authentifizierungsmethode beim Anlegen des Benutzers gewählt wurde, der sich an der Security-Baugruppe anmeldet, wird die Authentifizierung von verschiedenen Instanzen durchgeführt:

- Authentifizierungsmethode "Passwort": Die Authentifizierung wird von der Security-Baugruppe übernommen.
- Authentifizierungsmethode "RADIUS": Die Authentifizierung wird von einem RADIUS-Server übernommen. S≥V4.0

Zuweisung von Rollen zu benutzerspezifischen IP-Regelsätzen S≥V4.0

An SCALANCE S Baugruppen ab V4 ist auch die Zuweisung von benutzerspezifischen IP-Regelsätzen möglich, welchen Rollen zugeordnet sind. Damit ist es möglich, eine Gruppe von Benutzern für den Zugriff auf bestimmte IP-Adressen freizuschalten.

Wenn ein RADIUS-Server zur Benutzerauthentifizierung verwendet wird und dem benutzerspezifischen IP-Regelsatz eine Rolle zugewiesen wird, können auch solche Benutzer vom RADIUS-Server authentifiziert werden, die nicht auf der Security-Baugruppe projektiert sind. Diese Benutzer müssen auf dem RADIUS-Server oder einer separaten Datenbank hinterlegt und dort derjenigen Rolle zugeordnet sein, welche in SCT dem benutzerspezifischen IP-Regelsatz zugeordnet ist. Dieses Vorgehen hat den Vorteil, dass alle Benutzerdaten ausschließlich auf dem RADIUS-Server abgelegt werden.

Weitere Informationen zur Authentifizierung durch RADIUS-Server finden Sie in folgendem Kapitel:
Authentifizierung durch RADIUS-Server (Seite 78)

Benutzerspezifische IP-Regelsätze werden lokal genutzt - Vereinbarungen

Es gelten dieselben Vereinbarungen wie in folgendem Kapitel beschrieben:

- Globale Firewall-Regelsätze - Vereinbarungen (Seite 142)

4.3.3.1 Benutzerspezifische IP-Regelsätze anlegen und zuweisen

So erreichen Sie diese Funktion

1. Wählen Sie im Navigationsbereich den Ordner "Benutzerspezifische IP-Regelsätze".
2. Wählen Sie den Menübefehl "Einfügen" > "Firewall-Regelsatz".

3. Geben Sie die folgenden Daten ein:
   – Name: Projektweit eindeutige Bezeichnung des benutzerspezifischen IP-Regelsatzes. Der Name erscheint nach der Zuweisung des Regelsatzes in der lokalen Regelliste der Security-Baugruppe.
   – Beschreibung: Geben Sie eine Beschreibung für den benutzerspezifischen IP-Regelsatz ein.
4. Klicken Sie auf die Schaltfläche "Regel hinzufügen".
5. Tragen Sie der Reihe nach die Firewall-Regeln in die Liste ein.
   Beachten Sie die Parameterbeschreibung in folgendem Kapitel:
   – IP-Paketfilter-Regeln (Seite 151)

   Beachten Sie die Besonderheiten bei Firewall-Regeln, die für NAT-/NAPT-Regeln automatisch durch SCT erzeugt wurden:
   – Zusammenhang zwischen NAT-/NAPT-Router und benutzerspezifischer Firewall (Seite 186)
6. Weisen Sie dem benutzerspezifischen IP-Regelsatz einen Benutzer oder mehrere Benutzer und/oder eine Rolle oder mehrere Rollen zu. Die Zuweisung von Rollen an benutzerspezifische IP-Regelsätze ist nur für SCALANCE S V4 Baugruppen möglich.

Hinweis

Zuordnung von benutzerspezifischen IP-Regelsätzen

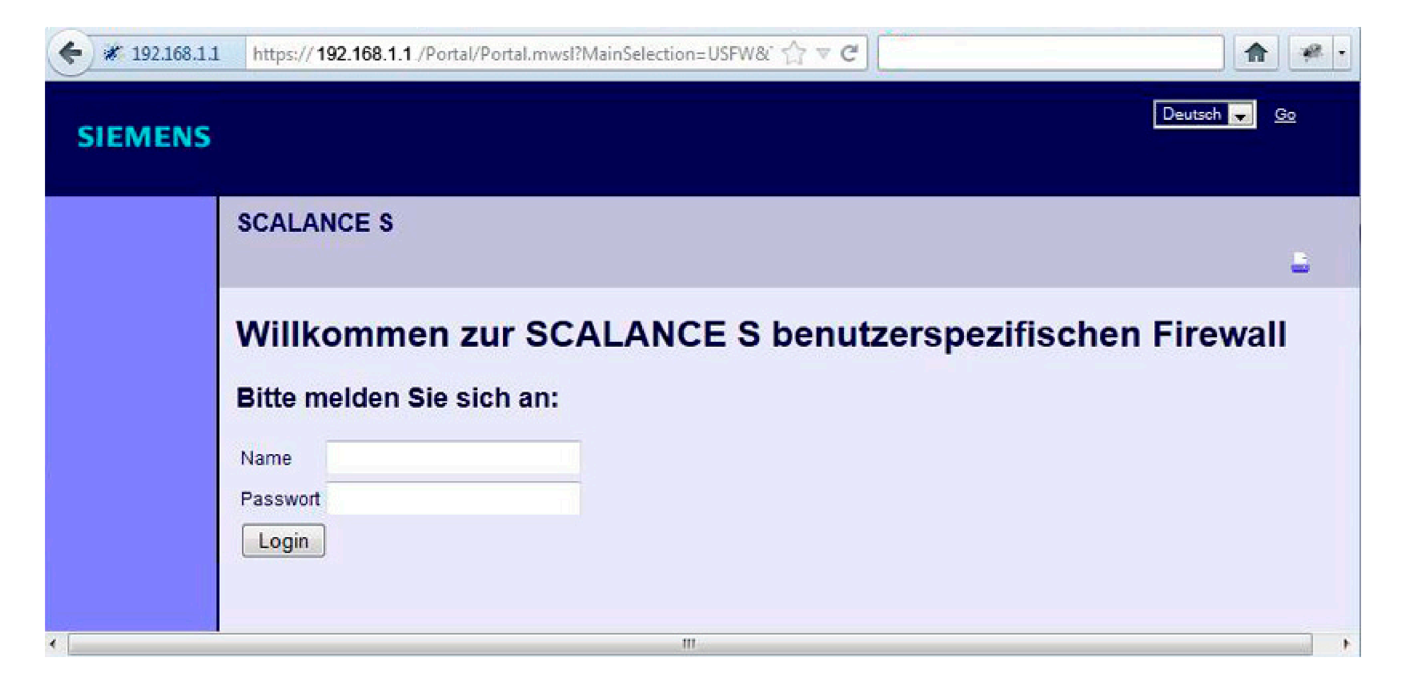
- Einer Security-Baugruppe kann nur ein benutzerspezifischer IP-Regelsatz pro Benutzer zugewiesen werden.
- Durch die Zuordnung wird für alle Benutzer bzw. Rollen, welche dem IP-Regelsatz zugeordnet sind, implizit das Recht "Benutzer/Rolle darf sich an Baugruppe anmelden" aktiviert.

---

7. Ordnen Sie den benutzerspezifischen IP-Regelsatz den Security-Baugruppen zu, in denen dieser verwendet werden sollen. Selektieren Sie dazu im Navigationsbereich den benutzerspezifischen IP-Regelsatz und ziehen Sie diesen auf die Security-Baugruppen im Navigationsbereich (Drag and Drop). Alternativ können Sie die Zuordnung in der lokalen Regelliste einer Security-Baugruppe über die Schaltfläche "Regelsätze hinzufügen..." vornehmen.

Ergebnis

- Der benutzerspezifische IP-Regelsatz wird von den Security-Baugruppen als lokaler Regelsatz verwendet und erscheint automatisch in der baugruppenspezifischen Liste der Firewall-Regeln.
- Der Benutzer kann sich an der Security-Baugruppe anmelden. Die Authentifizierung des Benutzers wird je nach eingestellter Authentifizierungsmethode von der Security-Baugruppe oder von einem RADIUS-Server durchgeführt.



Wertebereiche für maximale Sitzungsdauer

Die Zeitdauer, nach deren Ablauf der Benutzer automatisch abgemeldet wird, kann beim Anlegen oder Bearbeiten eines Benutzers festgelegt werden und beträgt standardmäßig 30 Minuten. Die Sitzungsdauer kann auf der Webseite der Security-Baugruppe auf den dem Benutzer zugewiesenen Wert verlängert werden.

Weitere Informationen zum Anlegen von Benutzern erhalten Sie in folgendem Kapitel: Benutzer verwalten (Seite 67)

4.3.4 Verbindungsbezogene automatische Firewall-Regeln



Automatisch angelegte Firewall-Regeln in SCT

Für folgenden Anwendungsfall werden automatisch Firewall-Regeln angelegt:

- In STEP 7 projektierte Verbindungen

Firewall-Regeln für projektierte Verbindungen

Sind in STEP 7 Verbindungen angelegt, werden für diese in SCT automatisch Firewall-Regeln erstellt. Dazu findet ein Systemabgleich zwischen STEP 7 und SCT statt, bei dem alle projektierten Verbindungen im Projekt überprüft werden. Automatisch abgeglichen werden für jeden Kommunikationspartner die IP-Adresse/MAC-Adresse, die Aktion und die Schnittstelle. Pro Kommunikationspartner entstehen unabhängig von der Anzahl der Verbindungen 2 Regeln.

Hinweis

UDP-Multicast- und UDP-Broadcast-Verbindungen manuell freigeben



Für UDP-Multicast- und UDP-Broadcast-Verbindungen werden keine automatischen Firewall-Regeln angelegt. Um die Verbindungen freizugeben, fügen Sie die entsprechenden Firewall-Regeln im Erweiterten Modus manuell hinzu.

Je nachdem, wie in STEP 7 der Verbindungsaufbau projektiert ist, werden in SCT die folgenden Ebene 3-Firewall-Regeln angelegt. Befindet sich die Security-Baugruppe in einer VPN-Gruppe, wechselt die Richtung "Extern" in "Tunnel".

In die Spalte "Quell-IP-Adresse" bzw. "Ziel-IP-Adresse" dieser Firewall-Regeln wird jeweils die IP-Adresse des Verbindungspartners eingetragen.

CP->extern	Aktion	Von	Nach
aktiv	Allow	Station	Extern
	Drop	Extern	Station
passiv	Drop	Station	Extern
	Allow	Extern	Station
aktiv und passiv	Allow	Extern	Station
	Allow	Station	Extern



CP->intern	Aktion	Von	Nach
aktiv	Allow	Station	Intern
	Drop	Intern	Station
passiv	Drop	Station	Intern
	Allow	Intern	Station
aktiv und passiv	Allow	Intern	Station
	Allow	Station	Intern

Für Ebene 2-Verbindungen werden "Allow"-Regeln für beide Richtungen angelegt. Befindet sich die Security-Baugruppe in einer VPN-Gruppe, wechselt die Richtung "Extern" in "Tunnel".

In die Spalte "Quell-MAC-Adresse" bzw. "Ziel-MAC-Adresse" dieser Firewall-Regeln wird jeweils die MAC-Adresse des Verbindungspartners eingetragen.

CP->extern	Aktion	Von	Nach
aktiv, passiv, aktiv und passiv	Allow	Station	Extern
	Allow	Extern	Station

Vereinbarungen für automatisch angelegte Firewall-Regeln

- Priorität

  Die Regeln haben die höchste Priorität und werden daher in der lokalen Regelliste oben eingefügt.

- Regeln löschen

  Die Regelsätze können nicht gelöscht werden. Das Logging kann aktiviert und Dienste können zugewiesen werden. Außerdem kann eine Bandbreite und ein Kommentar eingefügt werden.

- Aktion umstellen

  Stellen Sie in SCT die Aktion von "Allow" auf "Drop" oder umgekehrt um, werden diese beim erneuten Systemabgleich wieder überschrieben. Sollen die vorgenommenen Änderungen bestehen bleiben, wählen Sie als Aktion "Allow*" oder "Drop*". In diesem Fall wird nur die IP-Adresse/MAC-Adresse mit STEP 7 abgeglichen und Aktion und Richtung bleiben wie eingestellt bestehen. Einstellungen zu Logging, Dienst, Bandbreite und Kommentar bleiben bei einem erneuten Systemabgleich auch ohne das Umstellen der Aktion auf "Allow*" bzw. "Drop*" bestehen. Ist die zugehörige Verbindung in STEP 7 nicht vorhanden, wird die Regel aus der Liste entfernt.

Security-Baugruppe in VPN-Gruppe

Standardmäßig wird das Kontrollkästchen "Ausschließlich getunnelte Kommunikation" aktiviert. Deaktivieren Sie das Kontrollkästchen, kann zusätzlich zur Tunnelkommunikation zwischen Tunnelpartnern Kommunikation mit weiteren Netzwerkteilnehmern aufgebaut werden, zu welchen keine Tunnel bestehen.

- Die Kommunikation läuft außerhalb des Tunnels, wenn die Partneradresse zu einer im SCT bekannten Station gehört, zu der kein VPN-Tunnel projektiert ist.
- Die Kommunikation läuft durch den VPN-Tunnel, wenn die Partneradresse ein VPN-Endpunkt ist.
- Kann nicht eindeutig zugeordnet werden, ob eine Verbindung innerhalb oder außerhalb des VPN-Tunnels laufen soll, wird die Verbindung dem VPN-Tunnel zugeordnet und ein entsprechender Hinweis wird angezeigt. Die Zuordnung kann im Erweiterten Modus, z. B. durch Ändern der "Von"-Richtung "Tunnel" auf "Extern", angepasst werden. Damit diese Anpassung bei einem erneuten Systemabgleich nicht wieder überschrieben wird, muss die Aktion "Allow*" bzw. "Drop*" ausgewählt werden.

Hinweis

Soll sichergestellt werden, dass ausschließlich eine Kommunikation durch den Tunnel möglich ist, müssen Sie im erweiterten Firewall-Modus entsprechende Firewall-Regeln, z. B. für interne Teilnehmer oder NDIS-Adressen, anlegen.

Um für einen CP ausschließlich getunnelte Kommunikation zuzulassen, fügen Sie eine Regel mit den folgenden Einstellungen ein:

- "Aktion": "Drop"
- "Von": "Any"
- "Nach": "Extern"

Für CP 1628 fügen Sie eine Regel mit den folgenden Einstellungen ein:

- "Aktion": "Drop"
- "Von": "Station"
- "Nach": "Extern"

Zusätzlich müssen Sie bereits bestehende Firewall-Regeln, die ungetunnelte Kommunikation erlauben, entfernen.

4.3.5 Lokale IP-Paketfilter-Regeln einstellen

Mittels IP-Paketfilter-Regeln können Sie auf IP-Telegramme wie beispielsweise UDP-, TCP-, ICMP-Telegramme filtern.

Innerhalb einer IP-Paketfilter-Regel können Sie auf Dienst-Definitionen zurückgreifen und damit die Filterkriterien weiter eingrenzen. Wenn Sie keine Dienste angeben, gilt die IP-Paketfilter-Regel für alle Dienste.

Dialog für lokale IP-Paketfilter-Regeln öffnen

SCT: Markieren Sie die zu bearbeitende Security-Baugruppe und wählen den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall".

STEP 7: Klicken Sie im Register "Security" neben "Start der Security-Konfiguration" auf die Schaltfläche "Ausführen", Register "Firewall".

IP-Paketfilter-Regeln eintragen

Tragen Sie der Reihe nach die Firewall-Regeln in die Liste ein; beachten Sie die Parameterbeschreibung und die Beispiele im Folgekapitel oder in der Online-Hilfe.

Globale und benutzerspezifische Regelsätze nutzen

Globale Firewall-Regelsätze und benutzerspezifische IP-Regelsätze, die Sie der Security-Baugruppe zugewiesen haben, werden automatisch in die lokale Regelliste aufgenommen. Erscheint der zugewiesene Regelsatz am Ende der Regelliste, dann wird er mit der geringsten Priorität bearbeitet. Sie können die Priorität ändern, indem Sie die Position in der Regelliste verändern.

Die Online-Hilfe erläutert Ihnen die Bedeutung der einzelnen Schaltflächen.





4.3.6 IP-Paketfilter-Regeln

Die Bearbeitung von IP-Paketfilter-Regeln erfolgt anhand folgender Auswertungen:

- In der Regel eingetragene Parameter;
- Reihenfolge und der damit verbundenen Priorität der Regeln.

Parameter

Die Projektierung einer IP-Regel beinhaltet folgende Parameter:

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Aktion	Zulassungsfestlegung (Freigabe/Sperre)	• Allow Telegramme gemäß Definition zulassen. • Drop Telegramme gemäß Definition sperren. Für automatisch angelegte Verbindungsregeln: CP • Allow* • Drop* Wählen Sie diese Regeln, findet kein Abgleich mit STEP 7 statt. Geänderte Regeln werden in SCT also nicht überschrieben.
Von / Nach	Die zugelassenen Kommunikationsrichtungen.	Wird in den folgenden Tabellen beschrieben.
Quell-IP-Adresse	Quell-Adresse der IP-Pakete	Siehe folgender Abschnitt in diesem Kapitel: • IP-Paketfilter-Regeln (Seite 151) Alternativ können Sie symbolische Namen eingeben. **Hinweis zum Ghost-Modus** S602 ≥V3.1 Bei aktiviertem Ghost-Modus wird die IP-Adresse des internen Teilnehmers zur Laufzeit dynamisch von der Security-Baugruppe ermittelt. Je nach ausgewählter Richtung können Sie keine Eingaben in der Spalte "Quell-IP-Adresse" (bei Richtung "Von Intern nach Extern") bzw. in der Spalte "Ziel-IP-Adresse" (bei Richtung "Von Extern nach Intern") machen. Stattdessen wird die IP-Adresse durch den SCALANCE S selbst automatisch in die Firewall-Regel eingefügt.
Ziel-IP-Adresse	Ziel-Adresse der IP-Pakete	

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Dienst	Name des verwendeten IP-/ICMP-Dienstes oder der Dienstgruppe. Mit Hilfe der Dienst-Definitionen können Sie Paketfilter-Regeln definieren. Sie wählen hier einen der von Ihnen im Dialog IP-Dienste definierten Dienste: • IP-Dienste • ICMP-Dienste • Dienstgruppe mit enthaltenen IP- und/oder ICMP-Diensten Wenn Sie noch keine Dienste definiert haben oder einen weiteren Dienst definieren möchten, betätigen Sie die Schaltfläche "IP-Dienste..." (im Register "IP-Regeln") bzw. "MAC-Dienste..." (im Register "MAC-Regeln").	Die Klappliste bietet die projektierten Dienste und Dienstgruppen zur Auswahl an. Keine Angabe bedeutet: es wird kein Dienst geprüft, die Regel gilt für alle Dienste. **Hinweis**: Damit die vordefinierten IP-Dienste in der Klappliste erscheinen, aktivieren Sie diese zunächst im Standard Modus.
Bandbreite (Mbit/s)	Einstellmöglichkeit für eine Bandbreitenbegrenzung. Kann nur eingegeben werden, wenn bei Aktion "Allow" ausgewählt ist. Ein Paket passiert die Firewall, wenn die Pass-Regel zutrifft und die zulässige Bandbreite für diese Regel noch nicht überschritten worden ist.	CP x43-1 Adv. und SCALANCE S < V3.0: 0.001 ... 100 CP 1628 und SCALANCE S ≥ V3.0: 0.001 ... 1000 Für Regeln in globalen und benutzerspezifischen Regelsätzen: 0.001 ... 100
Logging	Ein- bzw. Ausschalten des Loggings für diese Regel. Informationen zu Logging-Einstellungen finden Sie in folgendem Kapitel: Ereignisse aufzeichnen (Logging) (Seite 261)	
Nr.	Automatisch vergebene Nummer der Regel zur Zuordnung der geloggten Pakete zu einer projektierten Firewall-Regel. Die Nummern werden beim Verschieben von Regeln neu ermittelt.	

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Stateful	Wenn dieses Kontrollkästchen für eine IP-Regel mit der Aktion "Allow" deaktiviert ist, werden durch Pakete, auf die die Allow-Regel zutrifft, keine Firewall-States erzeugt. Durch Firewall-States werden die Antworten auf zugelassene Pakete automatisch zugelassen. Kann nur angepasst werden, wenn bei Aktion "Allow" ausgewählt ist. Die Projektierung von IP-Regeln ohne Firewall-States ist nur für SCALANCE S Module ab Firmware V3 möglich. Sollen die Antworten auf Pakete, die die Firewall gemäß solcher IP-Regeln passiert haben, ebenfalls zugelassen werden, so müssen für diese Antworten zusätzliche IP-Regeln projektiert werden.	
Kommentar	Platz für eigene Erläuterung der Regel.	Ist ein Kommentar mit "AUTO" gekennzeichnet, wurde er automatisch für eine Verbindungsregel angelegt.

Tabelle 4- 11 Richtungen CP

Auswahlmöglichkeiten / Wertebereiche		Security-Baugruppe		Bedeutung
Von	Nach	CP x43-1 Adv.	CP 1628	
Intern	Station	x	-	Zugriff vom internen Netz auf die Station.
	Any	x	-	Zugriff vom internen auf das externe Netz, VPN-Tunnelpartner und die Station.
Extern	Station	x	x	Zugriff vom externen Netz auf die Station.
	Any	x	-	Zugriff vom externen auf das interne Netz und die Station.
Station	Intern	x	-	Zugriff von der Station auf das interne Netz.
	Extern	x	x	Zugriff von der Station auf das externe Netz.
	Tunnel	x	x	Zugriff von der Station auf VPN-Tunnelpartner.
Tunnel	Station	x	x	Zugriff über VPN-Tunnelpartner auf die Station.
	Any	x	-	Zugriff von VPN-Tunnelpartnern auf das interne Netz und die Station.
Any	Extern	x	-	Zugriff vom internen Netz und der Station auf das externe Netz.

Tabelle 4- 12 Richtungen SCALANCE S

Auswahlmöglichkeiten / Wertebereiche		Security-Baugruppe		
Von	Nach	S602	S61x	S623 / S627-2M
Intern	Extern	x	x	x

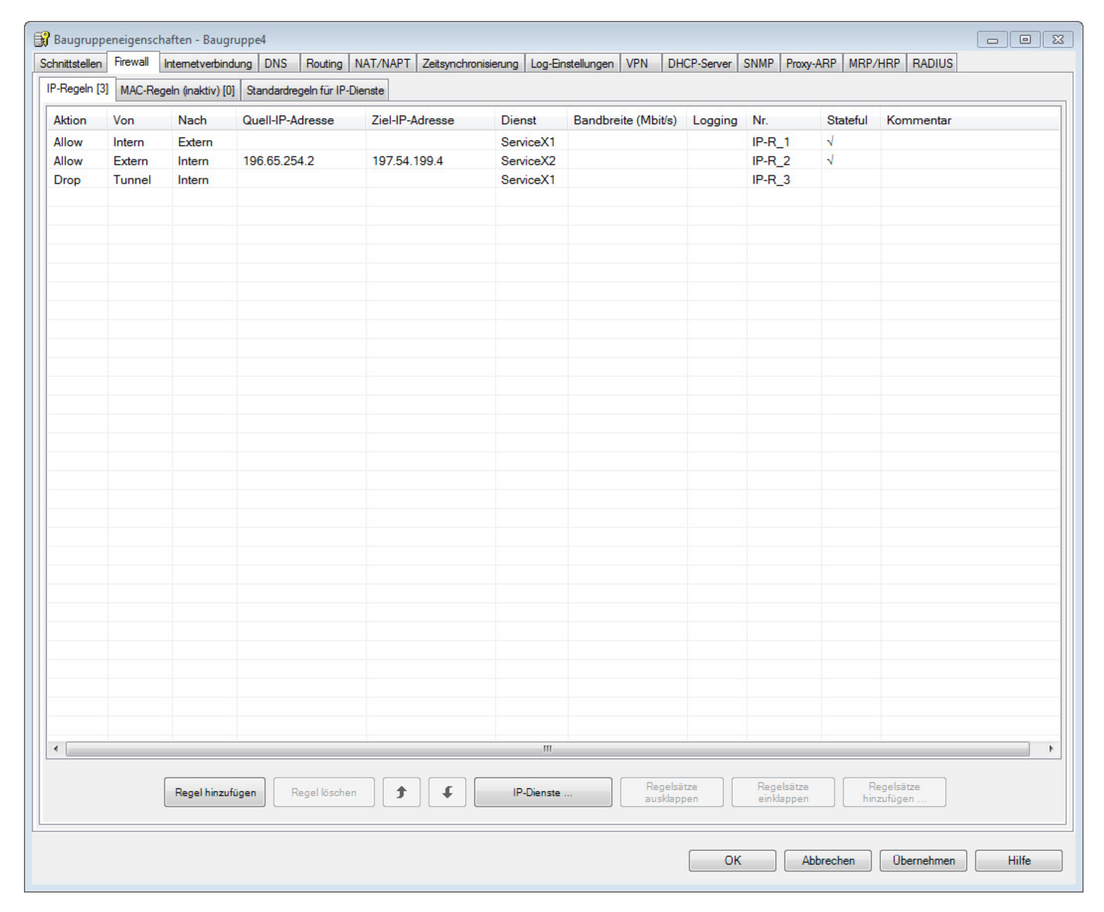
Auswahlmöglichkeiten / Wertebereiche		Security-Baugruppe		
	Tunnel	-	x	x
	Any	-	x	x
	DMZ	-	-	x
	Intern	x	x	x
Extern	Intern	x	x	x
	Any	-	-	x
	Tunnel	-	-	x
	DMZ	-	-	x
Tunnel	Intern	-	x	x
	Extern	-	x	x
	DMZ	-	-	x
Any	Intern	-	x	x
	Extern	-	-	x
	DMZ	-	-	x
DMZ	Intern	-	-	x
	Extern	-	-	x
	Any	-	-	x
	Tunnel	-	-	x

Reihenfolge bei der Regelauswertung durch die Security-Baugruppe

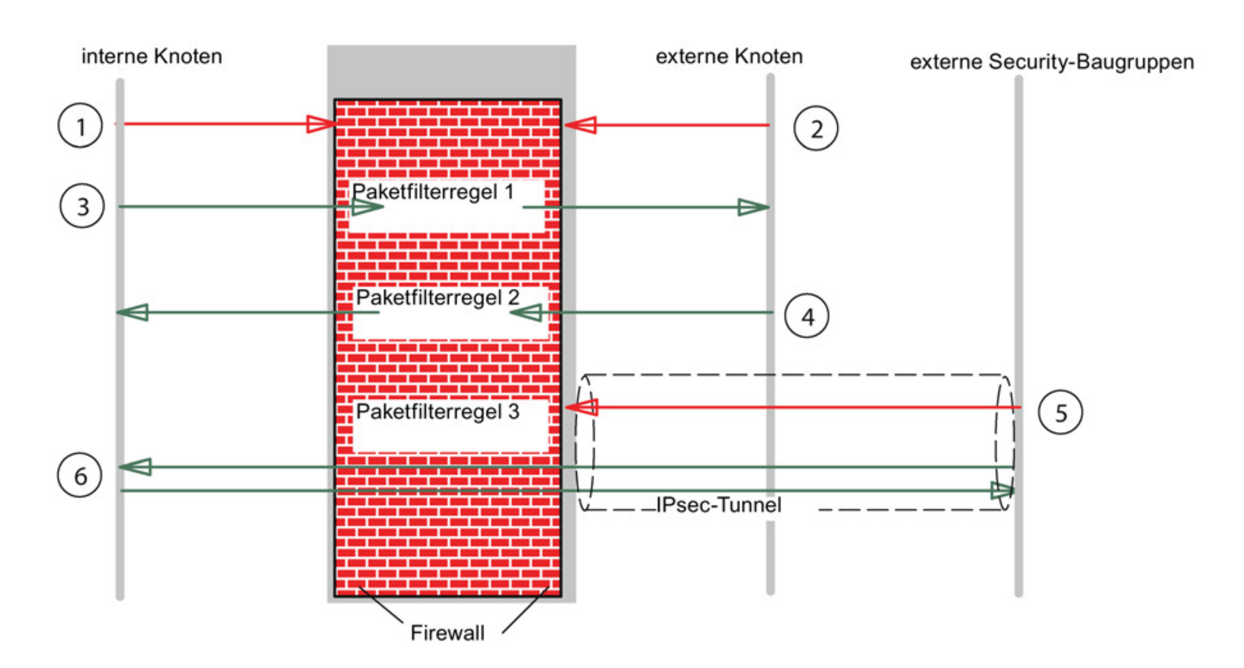
Die Paketfilter-Regeln werden wie folgt ausgewertet:

- Die Liste wird von oben nach unten ausgewertet; bei sich widersprechenden Regeln (z.B. Einträge mit gleichen Richtungsangaben, aber unterschiedlichen Aktionen) gilt also immer der weiter oben stehende Eintrag.
- Bei Regeln für die Kommunikation zwischen internem Netz, externem Netz und DMZ-Netz gilt: alle Telegramme außer den in der Liste explizit zugelassenen Telegrammen sind gesperrt.
- Bei Regeln für die Kommunikation in und aus Richtung IPsec-Tunnel gilt: alle Telegramme außer den in der Liste explizit gesperrten Telegrammen sind zugelassen.

Beispiel



Die dargestellten Paketfilter-Regeln bewirken folgendes Verhalten:



① Alle Telegrammtypen von intern nach extern sind standardmäßig geblockt, außer den explizit zugelassenen.

② Alle Telegrammtypen von extern nach intern sind standardmäßig geblockt, außer den explizit zugelassenen.

③ Die IP-Paketfilter-Regel 1 lässt Telegramme mit der Dienstdefinition "Service X1" von intern nach extern zu.

④ Die IP-Paketfilter-Regel 2 lässt Telegramme von extern nach intern zu, wenn erfüllt ist:

- IP-Adresse des Absenders: 196.65.254.2
- IP-Adresse des Empfängers: 197.54.199.4
- Dienstdefinition: "Service X2"

⑤ Die IP-Paketfilter-Regel 3 blockt Telegramme mit der Dienstdefinition "Service X1", die vom VPN-Tunnel ins interne Netz gesendet werden.

⑥ IPsec-Tunnelkommunikation ist standardmäßig zugelassen, außer den explizit geblockten Telegrammtypen.

Siehe auch

MAC-Paketfilter-Regeln (Seite 161)

Wertebereiche IP-Adresse, Subnetzmaske und Adresse des Netzübergangs (Seite 273)

IP-Adressen in IP-Paketfilter-Regeln

Die IP-Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; Beispiel: 141.80.0.16

In der Paketfilter-Regel haben Sie folgende Möglichkeiten, IP-Adressen anzugeben:

- keine Angabe

  Es erfolgt keine Prüfung, die Regel gilt für alle IP-Adressen.

- eine IP-Adresse

  Die Regel gilt genau für die angegebene Adresse.

- mehrere IP-Adressen

  Die Regel gilt für die angegebenen Adressen.

  Die Adressen werden getrennt durch ein Semikolon angegeben.
- Adressband

  Die Regel gilt für alle im Adressband erfassten IP-Adressen.

  Ein Adressband wird definiert, indem die Anzahl der gültigen Bit-Stellen in der IP-Adresse angegeben wird und zwar in der Form: [IP-Adresse]/[Anzahl der zu berücksichtigenden Bits]

  – [IP-Adresse]/24 bedeutet demnach, dass nur die höchstwertigen 24 Bit der IP-Adresse in der Filterregel berücksichtigt werden; das sind die ersten drei Stellen der IP-Adresse.

  – [IP-Adresse]/25 bedeutet, dass nur die ersten drei Stellen und das höchstwertige Bit der vierten Stelle der IP-Adresse in der Filterregel berücksichtigt werden.
- Adressbereich

  Für die Quell-IP-Adresse kann ein Adressbereich, getrennt durch einen Bindestrich, angegeben werden:

  [Start-IP-Adresse]-[End-IP-Adresse]

Nähere Informationen finden Sie in folgendem Kapitel:

- Wertebereiche IP-Adresse, Subnetzmaske und Adresse des Netzübergangs (Seite 273)

Tabelle 4- 13 Beispiele für Adressband bei IP-Adressen

Quell-IP-Adresse bzw. Ziel-IP-Adresse	**Adressband**		**Anzahl Adressen**
	von	**bis**	
192.168.0.0/**16**	192.168.0.0	192.168.255.255	65.536
192.168.10.0/**24**	192.168.10.0	192.168.10.255	256
192.168.10.0/**25**	192.168.10.0	192.168.10.127	128
192.168.10.0/**26**	192.168.10.0	192.168.10.63	64
192.168.10.0/**27**	192.168.10.0	192.168.10.31	32
192.168.10.0/**28**	192.168.10.0	192.168.10.15	16
192.168.10.0/**29**	192.168.10.0	192.168.10.7	8
192.168.10.0/**30**	192.168.10.0	192.168.10.3	4

4.3.7 IP-Dienste definieren

So erreichen Sie diese Funktion

- Über den Menübefehl "Optionen" > "IP-Dienste...".

  oder

- Aus dem Register "IP-Regeln" über die Schaltfläche "IP-Dienste...".

Bedeutung

Mit Hilfe der IP-Dienst-Definitionen können Sie Firewall-Regeln, die auf bestimmte Dienste angewendet werden, kompakt und übersichtlich definieren. Sie vergeben hierbei einen Namen und ordnen diesem die Dienstparameter zu.

Zusätzlich können Sie so definierte Dienste wiederum unter einem Gruppennamen zu Gruppen zusammenfassen.

Bei der Projektierung der globalen oder lokalen Paketfilter-Regeln verwenden Sie dann diese Namen.

Parameter für IP-Dienste

Die Definition der IP-Dienste erfolgt über folgende Parameter:

Tabelle 4- 14 IP-Dienste: Parameter

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Name	Frei definierbarer Name für den Dienst, der zur Identifikation in der Regeldefinition oder in der Gruppenzusammenfassung verwendet wird.	freie Eingabe
Protokoll	Name des Protokolltyps	TCP UDP Alle
Quell-Port	Es erfolgt eine Filterung anhand der hier angegebenen Portnummer; diese definiert den Dienstzugang beim Telegrammabsender.	Bei der Protokollauswahl "Alle" ist keine Portangabe möglich. Beispiele: *: Port wird nicht geprüft 20 bzw. 21: FTP-Service
Ziel-Port	Es erfolgt eine Filterung anhand der hier angegebenen Portnummer; diese definiert den Dienstzugang beim Telegrammempfänger.	Bei der Protokollauswahl "Alle" ist keine Portangabe möglich. Beispiele: *: Port wird nicht geprüft 80: Web-HTTP-Service 102: S7-Protokoll - TCP/Port

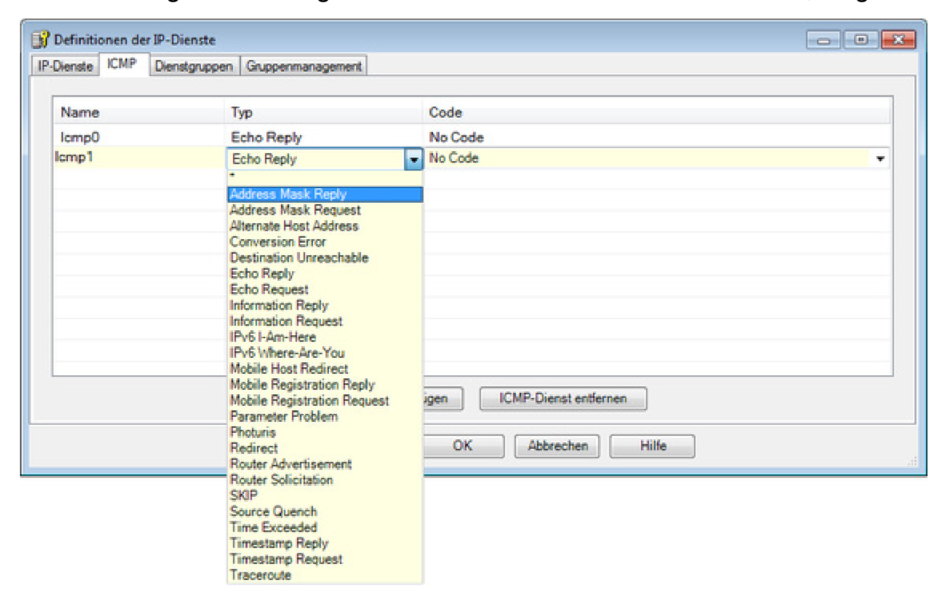
4.3.8 ICMP-Dienste definieren

Mit Hilfe der ICMP-Dienst-Definitionen können Sie Firewall-Regeln definieren, die auf bestimmte ICMP-Dienste angewendet werden. Sie vergeben hierbei einen Namen und ordnen diesem die Dienstparameter zu. Die definierten Dienste können Sie unter einem Gruppennamen zu Gruppen zusammenfassen. Bei der Projektierung der Paketfilter-Regeln verwenden Sie dann diese Gruppennamen.

So erreichen Sie diese Funktion

- Über den Menübefehl "Optionen" > "IP-Dienste...", Register "ICMP".

  oder
- Aus dem Register "IP-Regeln" über die Schaltfläche "IP-Dienste...", Register "ICMP"



Parameter für ICMP-Dienste

Die Definition der ICMP-Dienste erfolgt über folgende Parameter:

Tabelle 4- 15 ICMP-Dienste: Parameter

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Name	Frei definierbarer Name für den Dienst, der zur Identifikation in der Regeldefinition oder in der Gruppenzusammenfassung verwendet wird.	Freie Eingabe
Typ	Typ der ICMP-Message	Siehe Dialog-Darstellung.
Code	Codes des ICMP-Types	Werte sind abhängig vom gewählten Typ.

4.3.9 MAC-Paketfilter-Regeln einstellen

Mittels MAC-Paketfilter-Regeln können Sie auf MAC-Telegramme filtern.

Hinweis

Keine MAC-Regeln bei aktiviertem Routing-Modus

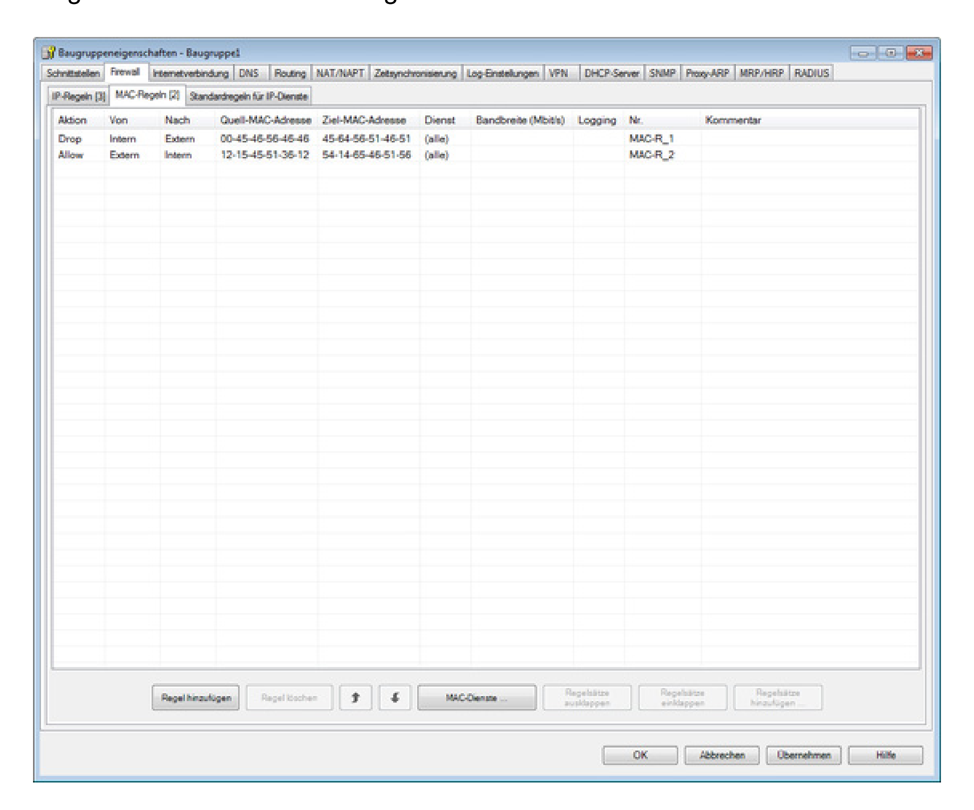


Wenn Sie für die SCALANCE S-Baugruppe den Routing-Modus aktiviert haben, finden MAC-Regeln keine Anwendung.

Dialog / Register

Markieren Sie die zu bearbeitende Security-Baugruppe.

Wählen Sie zum Einrichten der Firewall den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall > "MAC-Regeln".



Paketfilter-Regeln eintragen

Tragen Sie der Reihe nach die Firewall-Regeln in die Liste ein; beachten Sie die Parameterbeschreibung und die Beispiele im Folgekapitel oder in der Online-Hilfe.

Globale Firewall-Regelsätze nutzen

Globale Firewall-Regelsätze, die Sie der Security-Baugruppe zugewiesen haben, werden automatisch in die lokale Regelliste aufgenommen. Erscheint der zugewiesene Regelsatz am Ende der Regelliste, dann wird er mit der geringsten Priorität bearbeitet. Sie können die Priorität ändern, indem Sie die Position in der Regelliste verändern.



Die Online-Hilfe erläutert Ihnen die Bedeutung der einzelnen Schaltflächen.

4.3.10 MAC-Paketfilter-Regeln

Die Bearbeitung von MAC-Paketfilter-Regeln erfolgt anhand folgender Auswertungen:

- In der Regel eingetragene Parameter;
- Priorität der Regel innerhalb des Regelsatzes.

MAC-Paketfilter-Regeln

Die Projektierung einer MAC-Regel beinhaltet folgende Parameter:

Tabelle 4- 16 MAC-Regeln: Parameter

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Aktion	Zulassungsfestlegung (Freigabe/Sperre)	• Allow Telegramme gemäß Definition zulassen. • Drop Telegramme gemäß Definition sperren. Für automatisch angelegte Verbindungsregeln: CP • Allow* • Drop* Wählen Sie diese Regeln, findet kein Abgleich mit STEP 7 statt. Geänderte Regeln werden in SCT also nicht überschrieben.
Von / Nach	Die zugelassenen Kommunikationsrichtungen.	Werden in den folgenden Tabellen beschrieben.
Quell-MAC-Adresse	Quell-Adresse der MAC-Pakete	Alternativ können Sie symbolische Namen eingeben.
Ziel-MAC-Adresse	Ziel-Adresse der MAC-Pakete	
Dienst	Name des verwendeten MAC-Dienstes oder der Dienstgruppe. "Any" fasst die für den einzelnen Eintrag zugelassenen Richtungen zusammen.	Die Klappliste bietet die projektierten Dienste und Dienstgruppen zur Auswahl an. Keine Angabe bedeutet: es wird kein Dienst geprüft, die Regel gilt für alle Dienste. **Hinweis**: Damit die vordefinierten MAC-Dienste in der Klappliste erscheinen, aktivieren Sie diese zunächst im Standard Modus.
Bandbreite (Mbit/s)	Einstellmöglichkeit für eine Bandbreiten-Begrenzung. Kann nur eingegeben werden, wenn bei Aktion "Allow" ausgewählt ist. Ein Paket passiert die Firewall, wenn die Pass-Regel zutrifft und die zulässige Bandbreite für diese Regel noch nicht überschritten worden ist.	CP x43-1 Adv. und SCALANCE S ≤ V3.0: 0.001 ... 100 CP 1628 und SCALANCE S ≥ V3.0: 0.001 ... 1000 Für Regeln in globalen und benutzerspezifischen Regelsätzen: 0.001 ... 100
Logging	Ein- bzw. Ausschalten des Logging für diese Regel.	
Nr.	Automatisch vergebene Nummer zur Zuordnung zu einer projektierten Firewall-Regel. Die Nummern werden beim Verschieben von Regeln neu ermittelt.	
Kommentar	Platz für eigene Erläuterung der Regel	Ist ein Kommentare mit "AUTO" gekennzeichnet, wurde er für eine automatische Verbindungsregel angelegt.

Erlaubte Richtungen

Folgende Richtungen können eingestellt werden:

Tabelle 4- 17 Firewall-Richtungen CP

Auswahlmöglichkeiten / Wertebereiche		**Security-Baugruppe**		**Bedeutung**
Von	**Nach**	**CP x43-1 Adv.**	**CP 1628**	
Extern	Station	x	x	Zugriff vom externen Netz auf die Station.
Station	Extern	x	x	Zugriff von der Station auf das externe Netz.
	Tunnel	x	x	Zugriff von der Station auf VPN-Tunnelpartner.
Tunnel	Station	x	x	Zugriff über VPN-Tunnelpartner auf die Station.

Tabelle 4- 18 Firewall-Richtungen SCALANCE S

Auswahlmöglichkeiten / Wertebereiche		**Security-Baugruppe**		
Von	**Nach**	**S602**	**S61x**	**S623 / S627-2M**
Intern	Extern	x	x	x
	Tunnel	-	x	x
	Any	-	x	x
Extern	Intern	x	x	x
	Any	-	-	x
	Tunnel	-	-	x
Tunnel	Intern	-	x	x
	Extern	-	x	x
Any	Intern	-	x	x
	Extern	-	-	x

Regelauswertung durch die Security-Baugruppe

Die Paketfilter-Regeln werden wie folgt ausgewertet:

- Die Liste wird von oben nach unten ausgewertet; bei sich widersprechenden Regeln gilt der weiter oben stehende Eintrag.
- Bei den Regeln für die Kommunikation in Richtung "Extern" oder von Richtung "Extern" gilt für alle nicht explizit erfassten Telegramme: alle Telegramme sind gesperrt, außer den in der Liste explizit zugelassenen Telegrammen.
- Bei den Regeln für die Kommunikation in Richtung "Tunnel" oder von Richtung "Tunnel" gilt für alle nicht explizit erfassten Telegramme: alle Telegramme sind zugelassen, außer den in der Liste explizit gesperrten Telegrammen.

Hinweis

IP-Regeln greifen für IP-Pakete, MAC-Regeln greifen für Layer-2-Pakete

Für die Firewall können Sie sowohl IP-Regeln als auch MAC-Regeln definieren. Die Bearbeitung in der Firewall ist anhand des Ethertypes des Paketes geregelt.

IP-Pakete werden abhängig von den IP-Regeln weitergeleitet bzw. geblockt und Layer-2-Pakete werden abhängig von den MAC-Regeln weitergeleitet bzw. geblockt.

Es ist nicht möglich, ein IP-Paket mit Hilfe einer MAC-Firewall-Regel beispielsweise hinsichtlich einer MAC-Adresse zu filtern.

Beispiele

Das Beispiel für den IP-Paketfilter in Kapitel 5.4.3 (Seite 151) können Sie sinngemäß auf die MAC-Paketfilter-Regeln anwenden.

4.3.11 MAC-Dienste definieren

So erreichen Sie diese Funktion

- Über den Menübefehl "Optionen" > "MAC-Dienste...".

  oder
- Aus dem Register "MAC-Regeln" über die Schaltfläche "MAC-Dienste...".

Bedeutung

Mit Hilfe der MAC-Dienst-Definitionen können Sie Firewall-Regeln, die auf bestimmte Dienste angewendet werden, definieren. Sie vergeben einen Namen und ordnen diesem die Dienstparameter zu. Zusätzlich können Sie so definierte Dienste unter einem Gruppennamen zu Gruppen zusammenfassen. Bei der Projektierung der globalen oder lokalen Paketfilter-Regeln verwenden Sie dann diese Namen.

Parameter für MAC-Dienste

Eine MAC-Dienst Definition beinhaltet eine Kategorie protokoll-spezifischer MAC-Parameter:

Tabelle 4- 19 MAC-Dienste Parameter

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Name	Frei definierbarer Name für den Dienst, der zur Identifikation in der Regeldefinition oder in der Gruppenzusammenfassung verwendet wird.	freie Eingabe
Protokoll	Name des Protokolltyps: • ISO ISO bezeichnet Telegramme mit folgenden Eigenschaften: Lengthfield <= 05DC (hex), DSAP= userdefined SSAP= userdefined CTRL= userdefined • SNAP SNAP bezeichnet Telegramme mit folgenden Eigenschaften: Lengthfield <= 05DC (hex), DSAP=AA (hex), SSAP=AA (hex), CTRL=03 (hex), OUI=userdefined, OUI-Type=userdefined • PROFINET IO	• ISO • SNAP • PROFINET IO • 0x (Code-Eingabe)
DSAP	Destination Service Access Point: LLC-Empfänger-Adresse	
SSAP	Source Service Access Point: LLC-Sender-Adresse	
CTRL	LLC Control Field	
OUI	Organizationally Unique Identifier (die ersten 3 Bytes der MAC Adresse = Hersteller Identifizierung)	
OUI-Typ	Protokoll-Typ/Identifizierung	
*) Die Protokolleingaben 0800 (hex) und 0806 (hex) werden nicht akzeptiert, da diese Werte für IP- bzw. ARP-Telegramme gelten.		

Hinweis

Verarbeitung für S7-CPs



Es werden nur Einstellungen zu ISO-Frames mit DSAP=SSAP=FE (hex) verarbeitet. Andere Frame-Typen sind für S7-CPs nicht relevant und werden daher schon vor der Bearbeitung durch die Firewall verworfen.

Spezielle Einstellungen für SIMATIC NET Dienste

Verwenden Sie für die Filterung spezieller SIMATIC NET Dienste bitte die folgenden SNAP-Einstellungen:

- DCP (Primary Setup Tool):

  PROFINET IO
- SiCLOCK:

  OUI= 08 00 06 (hex), OUI-Type= 01 00 (hex)

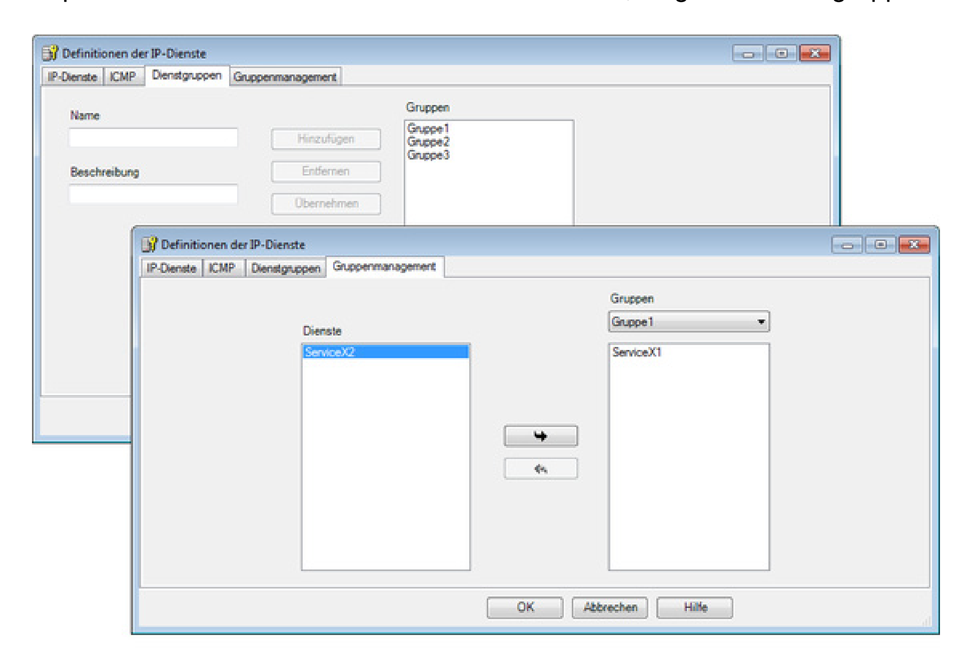
4.3.12 Dienstgruppen einrichten

Bildung von Dienstgruppen

Sie können mehrere Dienste durch die Bildung von Dienstgruppen zusammenzufassen. Auf diese Weise können Sie komplexere Dienste aufbauen, die in den Paketfilter-Regeln dann durch einfache Namensauswahl verwendet werden können.

Dialoge / Register

Sie öffnen den Dialog über folgenden Menübefehl:
"Optionen" > "IP-Dienste..." bzw. "MAC-Dienste...", Register "Dienstgruppen".



4.3.13 Standardregeln für IP-Dienste anpassen

So erreichen Sie diese Funktion:

1. Selektieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften..." > Register "Firewall" > Register "Standardregeln für IP-Dienste".

Bedeutung der erweiterten Einstellungen

Parameter	Bedeutung bei Aktivierung
Erweiterte Zustandsoptionen verwenden	Wenn Sie dieses Kontrollkästchen aktivieren, werden Verbindungen und Firewall-Zustände für Netzwerkteilnehmer begrenzt. Die Begrenzungen lauten: • Max. 200 Verbindungen in 5 Sekunden • Max. 2000 Firewall-Zustände Überschreitet ein Netzwerkteilnehmer eine dieser Begrenzungen, wird dessen IP-Adresse in die IP-Blacklist der Security-Baugruppe aufgenommen. Der Teilnehmer kann dann nicht mehr über die Security-Baugruppe kommunizieren. Die IP-Blacklist der Security-Baugruppe kann im Online-Modus eingesehen werden.
Alle aktivierten Regeln loggen	Pakete, die gemäß den Standardregeln für IP-Dienste zugelassen werden, werden geloggt.
ICMP-Test für Schnittstellen freischalten	Ping-Anfragen, die an einer Schnittstelle der Security-Baugruppe eingehen, können an andere Schnittstellen weitergeleitet werden. Aus dem externen Netz können somit beispielsweise Ping-Anfragen auf die interne Schnittstelle der Security-Baugruppe durchgeführt werden.

Bedeutung der standardmäßigen Firewall-Regeln

In diesem Dialog haben Sie die Möglichkeit, die dienstspezifischen Firewall-Regeln, die für die Schnittstellen der Security-Baugruppen standardmäßig eingestellt sind, anzupassen. Die standardmäßigen Einstellungen des Dialogs entsprechen den standardmäßigen Firewall-Regeln der jeweiligen Security-Baugruppe.

Standardmäßige Firewall-Regeln für SCALANCE S

In der folgenden Tabelle sind die standardmäßigen Firewall-Regeln für SCALANCE S Baugruppen aufgeführt. Die Firewall-Regeln sind zum Teil nur dann aktiv, wenn der betreffende Dienst von der Security-Baugruppe verwendet wird (z.B. SNMP).

Dienst	Richtung	Schnittstelle X1 (rot)	Schnittstelle X2 (grün)	Schnittstelle X3 (gelb) S62x	Tunnelschnitt-stelle S602
Schnittstellenrerouting	ausgehend	-	x	-	-
HTTPS		x	x*	x	x*
ICMP	eingehend	-	x	-	x
ICMP Pathfinder S602 ≥V3.1	ausgehend	-	x	-	-
SNMP	eingehend	x	x	x	x
Syslog	ausgehend	x	x	x	x
NTP	ausgehend	x	x	x	x
DNS	ausgehend	x	x	x	x
HTTP	ausgehend	x	-	x	-
VPN (IKE)		x	-	x	-
VPN (NAT Traversal)		x	-	x	-
BootP Server	eingehend	-	x	x	-
BootP Client	ausgehend	-	x	x	-
RADIUS	ausgehend	x	x	x	x
CARP S62x ≥ V4.0	ausgehend	x*	x*	-	-
Pfsync S62x ≥ V4.0	ausgehend	-	-	x*	-

x standardmäßig aktiviert

- standardmäßig deaktiviert

* nicht anpassbar

Standardmäßige Firewall-Regeln für S7-CPs

In der folgenden Tabelle sind die standardmäßigen Firewall-Regeln für S7-CPs aufgeführt. Die Firewall-Regeln sind nur dann eingestellt, wenn der betreffende Dienst im Security Configuration Tool aktiviert ist.

Dienst	Richtung	Extern (GBit)	Intern (PN-IO)
VPN (IKE)		x*	-*
VPN (NAT-Traversal)		x*	-*
BootP Server	ausgehend	x*	x*
BootP Client	eingehend	x*	x*

x standardmäßig aktiviert

- standardmäßig deaktiviert

* nicht anpassbar

Die beiden Dienste "BootP Server" und "BootP Client" sind jeweils entweder an der externen Schnittstelle oder an der internen Schnittstelle gemeinsam aktiv. Entsprechend sind entweder beide Firewall-Regeln an der externen Schnittstelle oder beide Firewall-Regeln an der internen Schnittstelle aktiv.

Weitere Baugruppeneigenschaften projektieren 5

5.1 Security-Baugruppe als Router

5.1.1 Übersicht

Bedeutung

Indem Sie die Security-Baugruppe als Router betreiben, werden die Netze an interner, externer und DMZ-Schnittstelle (nur SCALANCE S623/S627-2M, siehe Abschnitt unten) zu separaten Subnetzen.

Sie haben folgende Möglichkeiten:

- Routing - einstellbar im Standard Modus und im Erweiterten Modus
- NAT/NAPT-Routing - einstellbar im Erweiterten Modus

Alle nicht zu einem Subnetz gehörenden Netzwerkanfragen werden durch einen Router in ein anderes Subnetz weitergeleitet, siehe folgendes Kapitel:

- Standard-Router und Routen festlegen (Seite 172)

Routing-Modus oder DMZ-Schnittstelle aktivieren - Register "Schnittstellen"



Wenn sie den Routing-Modus oder die DMZ-Schnittstelle aktiviert haben, werden die Telegramme weitergeleitet, die an eine im jeweiligen Subnetz (intern, extern, DMZ) vorhandene IP-Adresse gerichtet sind. Darüber hinaus gelten die für die jeweilige Übertragungsrichtung projektierten Firewall-Regeln.

Für diese Betriebsart müssen Sie im Register "Schnittstellen" für die interne Schnittstelle und/oder für die DMZ-Schnittstelle eine IP-Adresse und eine Subnetzmaske für die Adressierung des Routers am internen Subnetz und/oder am DMZ-Subnetz projektieren. Alle nicht zu einem Subnetz gehörenden Netzwerkanfragen werden durch den Standard-Router in ein anderes Subnetz weitergeleitet.

Hinweis

Im Gegensatz zum Bridge-Betrieb der Security-Baugruppe gehen im Routing-Modus VLAN-Tags verloren.

Bridge- und Routing-Modus bei SCALANCE S623/S627-2M

Bei dem DMZ-Netz handelt es sich stets um ein separates Subnetz. Der Unterschied zwischen dem Bridge-Modus und dem Routing-Modus liegt in der Unterteilung des externen und internen Netzes:

- Betriebsart "Bridge": Internes und externes Netz befinden sich im gleichen Subnetz; DMZ-Netz befindet sich in separatem Subnetz.
- Betriebsart "Routing": Internes und externes Netz befinden sich jeweils in einem eigenen Subnetz; DMZ-Netz befindet sich in einem weiteren, separaten Subnetz.

5.1.2 Standard-Router und Routen festlegen

So erreichen Sie diese Funktion

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Routing".
3. Wenn Sie die IP-Adresse / den FQDN für den Standard-Router eintragen, werden alle Routen über diesen Router geleitet, sofern keine spezifischen Routen zutreffen. Spezifische Routen können Sie im Eingabebereich "Routen" eintragen.
4. Klicken Sie auf die Schaltfläche "Route hinzufügen".
5. Tragen Sie die folgende Werte ein:

Parameter	Funktion	Beispiel-Wert
Netz-ID	Anfragen an Teilnehmer des Subnetzes mit der hier angegebenen Netz-ID und der angegebenen Subnetzmaske werden über die angegebene Router-IP-Adresse in das Subnetz geleitet. Anhand der Netz-ID erkennt der Router, ob eine Ziel-Adresse im oder außerhalb des Subnetzes liegt. Die angegebene Netz-ID darf nicht im gleichen Subnetz liegen wie die IP-Adresse der Security-Baugruppe.	192.168.11.0
Subnetzmaske	Die Subnetzmaske strukturiert das Netz. Anhand der Netz-ID und der Subnetzmaske erkennt der Router, ob eine Ziel-Adresse innerhalb oder außerhalb des Subnetzes liegt. Die anzugebende Subnetzmaske kann nicht auf einen einzelnen Netzwerkteilnehmer beschränkt werden (255.255.255.255).	255.255.255.0
Router-IP-Adresse	IP-Adresse / FQDN des Routers, über den das Subnetz erreicht wird. Die IP-Adresse des Routers muss im gleichen Subnetz liegen wie die IP-Adresse der Security-Baugruppe.	192.168.10.2 / my-router.dyndns.org
Rerouting aktivieren (nur für SCALANCE S V3/V4 Baugruppen)	Aktivieren Sie dieses Kontrollkästchen, wenn die Telegramme der eingegebenen Route an derselben Schnittstelle der Security-Baugruppe ein- und ausgehen sollen (Rerouting). Rerouting wird nur an der internen Schnittstelle der Security-Baugruppe unterstützt.	

Besonderheiten beim Standard-Router

S≥V3.0

- Ist im Register "Schnittstellen" die IP-Zuweisung über "PPPoE" konfiguriert, wird ein projektierter Standard-Router ignoriert, da die Standard-Route automatisch immer über die PPPoE-Schnittstelle führt.
- Ist im Register "Schnittstellen" die Adresszuweisung über "Statische Adresse" konfiguriert und ist die Security-Baugruppe über einen DSL-(NAPT-) Router am Internet angeschlossen, muss der DSL-Router als Standard-Router eingetragen werden.
- Für Security-Baugruppen im Ghost-Modus (nur SCALANCE S602 ≥ V3.1) sind keine Standard-Router projektierbar, da diese zur Laufzeit ermittelt werden. Spezifische Routen sind für Security-Baugruppen im Ghost-Modus nicht projektierbar.

5.1.3 NAT-/NAPT-Routing



Voraussetzung

- Das Projekt befindet sich im Erweiterten Modus.
- Die Security-Baugruppe befindet sich im Routing-Modus oder die DMZ-Schnittstelle (nur SCALANCE S623 / S627-2M) ist aktiviert.

So erreichen Sie diese Funktion

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "NAT/NAPT".
3. Aktivieren Sie je nach Anforderung eine Adressumsetzung gemäß NAT (Network Address Translation) oder NAPT (Network Address Port Translation).

Adressumsetzung mit NAT (Network Adress Translation)

NAT ist ein Protokoll zur Adressumsetzung zwischen zwei Adressräumen. Hauptaufgabe ist die Umsetzung von privaten IP-Adressen in öffentliche, d. h. in IP-Adressen, die im Internet verwendet und auch geroutet werden. Dadurch wird erreicht, dass die IP-Adressen des internen Netzes nach außen im externen Netz nicht bekannt werden. Die internen Teilnehmer sind im externen Netz nur über die in der Adressumsetzungsliste (NAT-Tabelle) festgelegten externen IP-Adressen sichtbar. Handelt es sich bei der externen IP-Adresse nicht um die Adresse der Security-Baugruppe und ist die interne IP-Adresse eindeutig, wird dies als 1:1 NAT bezeichnet. Beim 1:1 NAT wird die interne Adresse ohne Portumsetzung auf diese externe Adresse umgesetzt. Ansonsten handelt es sich um n:1 NAT.

Adressumsetzung mit NAPT (Network Address Port Translation)

Die Adressumsetzung bei NAPT verändert die Ziel-IP-Adresse und den Ziel-Port in einer Kommunikationsbeziehung (Portweiterleitung).

Umgesetzt werden Telegramme, die vom externen Netz oder vom DMZ-Netz kommen und an die IP-Adresse der Security-Baugruppe gerichtet sind. Ist der Ziel-Port des Telegramms identisch mit einem der Werte, der in der Spalte "Quell-Port" angegeben ist, so ersetzt die Security-Baugruppe die Ziel-IP-Adresse und den Ziel-Port, wie in der entsprechenden Zeile der NAPT-Tabelle angegeben. Bei der Rückantwort setzt die Security-Baugruppe als Quell-IP-Adresse und als Quell-Port die Werte ein, die beim Initialtelegramm als Ziel-IP-Adresse bzw. Ziel-Port stehen.

Der Unterschied zu NAT liegt darin, dass bei diesem Protokoll auch Ports umgesetzt werden können. Es gibt keine 1:1 Umsetzung der IP-Adresse. Vielmehr existiert nur noch eine öffentliche IP-Adresse, die durch den Zusatz von Portnummern an eine Reihe von privaten IP-Adressen umgesetzt wird.

Adressumsetzung in VPN-Tunneln

Adressumsetzungen mit NAT/NAPT können auch für Kommunikationsbeziehungen durchgeführt werden, welche über VPN-Tunnel aufgebaut werden. Dies wird für die Verbindungspartner vom Typ SCALANCE M (nur 1:1-NAT) und SCALANCE S612 / S623 / S627-2M V4 unterstützt.

Weitere Informationen zu Adressumsetzungen in VPN-Tunneln finden Sie in folgenden Kapiteln:

- Adressumsetzung mit NAT/NAPT (Seite 175)
- Adressumsetzung mit NAT/NAPT in VPN-Tunneln (Seite 182)

Konvertierung von NAT-/NAPT-Regeln aus Altprojekten

Mit SCT V4.0 wurde der Projektierungsmodus von NAT-/NAPT-Regeln und der zugehörigen Firewall-Regeln geändert. Wenn Sie die NAT-/NAPT-Regeln aus einem Projekt, das mit SCT V3.0/V3.1 erstellt wurde, in SCT V4.0 anpassen oder erweitern wollen, müssen Sie zunächst die NAT-/NAPT-Regeln nach SCT V4.0 konvertieren. Wählen Sie hierzu im Kontextmenü einer NAT-/NAPT-Regel den Menübefehl "Alle NAT-/NAPT-Regeln nach SCT V4 konvertieren" bzw. "Gewählte NAT-/NAPT-Regel nach SCT V4 konvertieren". Für die konvertierten NAT-/NAPT-Regeln werden daraufhin von SCT automatisch Firewall-Regeln erzeugt, die die Kommunikation in der projektierten Adressumsetzungsrichtung freigeben. Ändern bzw. Entfernen Sie im Anschluss die Firewall-Regeln, die Sie manuell für die NAT-/NAPT-Regeln erzeugt haben, sofern diese im Widerspruch zu den automatisch erzeugten Firewall-Regeln stehen. Führen Sie dann die gewünschten Anpassungen und/oder Erweiterungen an den NAT-/NAPT- und Firewall-Regeln durch.

Konsistenzprüfung - diese Regeln müssen Sie beachten

Beachten Sie unter anderem folgende Regeln, um konsistente Einträge zu erhalten:

- Die IP-Adresse der internen Schnittstelle darf nicht in der NAT-/NAPT-Tabelle verwendet werden.
- Eine IP-Adresse, die in der NAT/NAPT-Adressumsetzungsliste verwendet wird, darf keine Multicast-Adresse und keine Broadcast-Adresse sein.
- Die für die NAPT-Umsetzung vergebenen externen Ports liegen im Bereich > 0 und ≤ 65535.

  Port 123 (NTP), 443 (HTTPS), 514 (Syslog), 161 (SNMP), 67+68 (DHCP) und 500+4500 (IPsec) sind davon ausgeschlossen, sofern die jeweiligen Dienste auf der Security-Baugruppe aktiviert sind.
- Die externe IP-Adresse der Security-Baugruppe bzw. die IP-Adresse der DMZ-Schnittstelle darf in der NAT-Tabelle nur für die Aktion "Source-NAT" verwendet werden.
- Duplikatsprüfung in der NAT-Tabelle

  Eine externe IP-Adresse bzw. eine IP-Adresse im DMZ-Netz, die mit Richtung "Destination-NAT", "Source-NAT + Destination-NAT" oder "Double-NAT" verwendet wird, darf in jeder angegebenen Richtung nur einmal verwendet werden.
- Duplikatsprüfung in der NAPT-Tabelle
  - Eine Quell-Portnummer darf für jede Schnittstelle nur einmal eingetragen sein.
  - Die Portnummern bzw. Portbereiche der externen Ports und der DMZ-Ports dürfen sich nicht überschneiden.
- Interne NAPT-Ports können im Bereich > 0 und ≤ 65535 liegen.

Führen Sie nach Abschluss Ihrer Eingaben eine Konsistenzprüfung durch.

Wählen Sie hierzu den Menübefehl "Optionen" > "Konsistenzprüfungen".

5.1.4 Adressumsetzung mit NAT/NAPT

NAT aktivieren

Der Eingabebereich für NAT wird aktiviert. NAT-Adressumsetzungen werden erst durch die nachfolgend beschriebenen Einträge in die Adressumsetzungsliste wirksam. Nach dem Anlegen von NAT-Regeln werden die zugehörigen Firewall-Regeln erzeugt und im Erweiterten Modus angezeigt, siehe Kapitel:
Zusammenhang zwischen NAT-/NAPT-Router und Firewall (Seite 184)

Wenn für die externe Schnittstelle oder die DMZ-Schnittstelle PPPoE aktiviert ist, kann die Aktion "Destination-NAT" nicht projektiert werden. Bei der Projektierung der Aktion "Source-NAT" kann die IP-Adresse im Eingabefeld "Quell-Umsetzung" nicht eingegeben werden, da diese dynamisch zur Laufzeit ermittelt wird.

Mögliche Adressumsetzungsaktionen für NAT

In den folgenden Tabellen sind die Eingabemöglichkeiten zur Adressumsetzung mit NAT dargestellt.

Aktion "Destination-NAT" - "Redirect"

Die Aktion "Destination-NAT" kann in folgender Richtung durchgeführt werden:

- Extern nach Intern

Wenn die DMZ-Schnittstelle der Security-Baugruppe (nur SCALANCE S623/S627-2M) aktiviert ist, kann die Aktion "Destination-NAT" zusätzlich in folgenden Richtungen durchgeführt werden:

- Extern nach DMZ
- DMZ nach Intern
- DMZ nach Extern

Wenn sich die SCALANCE S Baugruppe in einer VPN-Gruppe (nicht für SCALANCE S602) befindet, kann die Aktion "Destination-NAT" zusätzlich in folgenden Richtungen durchgeführt werden:

- Tunnel nach Intern
- Tunnel nach Extern
- Tunnel nach DMZ (nur bei aktivierter DMZ-Schnittstelle)

Für die Richtung "Extern nach Intern" gilt beispielsweise: Die Ziel-IP-Adresse eines vom externen Netz kommenden Telegramms wird auf Übereinstimmung mit der IP-Adresse geprüft, die im Eingabefeld "Ziel-IP-Adresse" angegeben ist. Bei Übereinstimmung wird das Telegramm in das interne Netz weitergeleitet, indem die Ziel-IP-Adresse des Telegramms durch die IP-Adresse ersetzt wird, die im Eingabefeld "Ziel-Umsetzung" angegeben ist. Der Zugriff von Extern nach Intern über die externe IP-Adresse ist möglich.

Die folgende Tabelle zeigt das Eingabeschema für die Aktion "Destination-NAT".

Feld	Mögliche Eingaben	Bedeutung
Quell-IP-Adresse	Für diese Aktion nicht relevant.	-
Quell-Umsetzung	Für diese Aktion nicht relevant.	-

Feld	Mögliche Eingaben	Bedeutung
Ziel-IP-Adresse	IP-Adresse im Quell-Netz	Ziel-IP-Adresse im Quell-Netz, über die auf eine IP-Adresse im Ziel-Netz zugegriffen werden soll. Die Ziel-IP-Adresse darf nicht mit der IP-Adresse der Security-Baugruppe im Quell-Netz übereinstimmen. Stimmt in einem Telegramm die Ziel-IP-Adresse mit der eingegebenen Adresse überein, wird die Adresse durch die entsprechende IP-Adresse im Ziel-Netz ausgetauscht. Die angegebene Ziel-IP-Adresse wird zur Alias-Adresse. Dies bedeutet, dass die angegebene IP-Adresse zusätzlich als IP-Adresse an der ausgewählten Schnittstelle registriert wird. Alias-Adressen werden zusätzlich im Register "Schnittstellen" der Security-Baugruppe angezeigt. Stellen Sie sicher, dass mit der Alias-Adresse kein IP-Adresskonflikt im Netzwerk besteht.
Ziel-Umsetzung	IP-Adresse im Ziel-Netz	Die Ziel-IP-Adresse wird durch die hier angegebene IP-Adresse ersetzt.
Nr.	-	Von SCT vergebene, fortlaufende Nummer, die zur Bezugnahme auf die Firewall-Regel verwendet wird, welche von SCT für die NAT-Regel erzeugt wird.

Aktion "Source-NAT" - "Masquerading"

Die Aktion "Source-NAT" kann in folgender Richtung durchgeführt werden:

- Intern nach Extern

Wenn die DMZ-Schnittstelle der Security-Baugruppe (nur SCALANCE S623/S627-2M) aktiviert ist, kann die Aktion "Source-NAT" zusätzlich in folgenden Richtungen durchgeführt werden:

- Intern nach DMZ
- Extern nach DMZ
- DMZ nach Extern

Wenn sich die SCALANCE S Baugruppe in einer VPN-Gruppe (nicht für SCALANCE S602) befindet, kann die Aktion "Source-NAT" zusätzlich in folgenden Richtungen durchgeführt werden:

- Intern nach Tunnel
- Extern nach Tunnel
- DMZ nach Tunnel (nur bei aktivierter DMZ-Schnittstelle)

Für die Richtung "Intern nach Extern" gilt beispielsweise: Die Quell-IP-Adresse eines vom internen Netz kommenden Telegramms wird auf Übereinstimmung mit der IP-Adresse geprüft, die im Eingabefeld "Quell-IP-Adresse" angegeben ist. Bei Übereinstimmung wird das Telegramm mit der im Eingabefeld "Quell-Umsetzung" angegebenen externen IP-Adresse als neue Quell-IP-Adresse in das externe Netz weitergeleitet. Am externen Netz wirkt die externe IP-Adresse.

Die folgende Tabelle zeigt das Eingabeschema für die Aktion "Source-NAT".

Feld	Mögliche Eingaben	Bedeutung
Quell-IP-Adresse	IP-Adresse im Quell-Netz	Die Quell-IP-Adresse des angegebenen Teilnehmers wird durch die im Eingabefeld "Quell-Umsetzung" angegebene IP-Adresse ersetzt.
	IP-Adressbereich / IP-Adressband im Quell-Netz	Die IP-Adressen des IP-Adressbereichs / des IP-Adressbands werden durch die im Eingabefeld "Quell-Umsetzung" angegebene IP-Adresse ersetzt.
Quell-Umsetzung	IP-Adresse im Ziel-Netz	Eingabe der IP-Adresse, die als neue Quell-IP-Adresse verwendet werden soll. Handelt es bei der hier eingegebenen IP-Adresse nicht um die IP-Adresse der Security-Baugruppe, wird diese zur Alias-Adresse. Dies bedeutet, dass die angegebene Adresse zusätzlich als IP-Adresse an der ausgewählten Schnittstelle registriert wird. Alias-Adressen werden zusätzlich im Register "Schnittstellen" der Security-Baugruppe angezeigt. Stellen Sie sicher, dass mit der Alias-Adresse kein IP-Adresskonflikt im Netzwerk besteht.
Ziel-IP-Adresse	Für diese Aktion nicht relevant.	Für diese Aktion nicht relevant.
Ziel-Umsetzung	Für diese Aktion nicht relevant.	Für diese Aktion nicht relevant.
Nr.	-	Von SCT vergebene, fortlaufende Nummer, die zur Bezugnahme auf die Firewall-Regel verwendet wird, welche von SCT für die NAT-Regel erzeugt wird.

Hinweis

Sie können für alle von einem Quell-Netz in ein Ziel-Netz gehenden Telegramme eine Adressumsetzung auf die Baugruppen-IP-Adresse im Ziel-Netz projektieren. Zusätzlich wird von der Security-Baugruppe an jedes Telegramm eine Port-Nummer vergeben. Es handelt sich hierbei um eine n:1-NAT-Adressumsetzung, bei welcher mehrere IP-Adressen des Quell-Netzes auf eine IP-Adresse des Ziel-Netzes umgesetzt werden.

Geben Sie beispielsweise für die Richtung "Intern nach Extern" die folgenden Parameter ein:

- Aktion: "Source-NAT"
- Von: "Intern"
- Nach "Extern"
- Quell-IP-Adresse: "*"
- Quell-Umsetzung: Externe IP-Adresse der Security-Baugruppe

Aktion "Source-NAT + Destination-NAT" - "1:1-NAT"

Die Aktion "Source-NAT + Destination-NAT" kann in folgender Richtung durchgeführt werden:

- Intern nach Extern

Wenn die DMZ-Schnittstelle der Security-Baugruppe (nur SCALANCE S623/S627-2M) aktiviert ist, kann die Aktion "Source-NAT + Destination-NAT" zusätzlich in folgenden Richtungen durchgeführt werden:

- Intern nach DMZ
- Extern nach DMZ
- DMZ nach Extern

Wenn sich die SCALANCE S Baugruppe in einer VPN-Gruppe (nicht für SCALANCE S602) befindet, kann die Aktion "Source-NAT + Destination-NAT" zusätzlich in folgenden Richtungen durchgeführt werden:

- Extern nach Tunnel
- Intern nach Tunnel
- DMZ nach Tunnel (nur bei aktivierter DMZ-Schnittstelle)

Für die Richtung "Intern nach Extern" gilt beispielsweise: Beim Zugriff von Intern nach Extern wird die Aktion "Source-NAT" durchgeführt. Beim Zugriff von Extern nach Intern wird die Aktion "Destination-NAT" durchgeführt.

Die folgende Tabelle zeigt das Eingabeschema für die Aktion "Source-NAT + Destination-NAT":

Feld	Mögliche Eingaben	Bedeutung
Quell-IP-Adresse	IP-Adresse im Quell-Netz	Die Projektierung wird immer in Source-NAT-Richtung angegeben. Die IP-Adressen der Destination-NAT-Richtung werden daraufhin automatisch von SCT eingefügt.
	IP-Adressbereich im Quell-Netz	
Quell-Umsetzung	IP-Adresse im Ziel-Netz	
Ziel-IP-Adresse	Für diese Aktion nicht relevant.	
Ziel-Umsetzung	Für diese Aktion nicht relevant.	
Nr.	-	Von SCT vergebene, fortlaufende Nummer, die zur Bezugnahme auf die Firewall-Regeln verwendet wird, welche von SCT für die NAT-Regel erzeugt werden.

Aktion "Double-NAT"

Die Aktion "Double-NAT" kann für SCALANCE S Baugruppen in folgenden Richtungen durchgeführt werden:

- Intern nach Extern
- Extern nach Intern

Wenn die DMZ-Schnittstelle der Security-Baugruppe (nur SCALANCE S623/S627-2M) aktiviert ist, kann die Aktion "Double-NAT" zusätzlich in folgenden Richtungen durchgeführt werden:

- Intern nach DMZ
- Extern nach DMZ
- DMZ nach Intern
- DMZ nach Extern

In jeder Richtung findet immer Source- und Destination-NAT zugleich statt.
Für die Richtung "Extern nach Intern" gilt beispielsweise: Beim Zugriff von Extern nach Intern wird die Quell-IP-Adresse des externen Teilnehmers ausgetauscht (Source-NAT). Zudem erfolgt der Zugriff auf das interne Netz über die im Eingabefeld "Ziel-IP-Adresse" angegebene externe IP-Adresse (Destination-NAT).

Sie können diese Aktion beispielsweise dann verwenden, wenn für ein Gerät, auf das mit Hilfe von Destination-NAT zugegriffen wird, ein anderer Standard-Router als die Security-Baugruppe eingetragen ist. Antworttelegramme von diesem Gerät werden dann nicht an den eingetragenen Standard-Router, sondern an die zugehörige Schnittstelle der Security-Baugruppe gesendet.

Die folgende Tabelle zeigt das Eingabeschema für die Aktion "Double-NAT":

Feld	Mögliche Eingaben	Bedeutung
Quell-IP-Adresse	IP-Adresse im Quell-Netz	IP-Adresse des Teilnehmers im Quell-Netz
Quell-Umsetzung	-	Die Source-NAT-Adressumsetzung erfolgt immer auf die IP-Adresse der Security-Baugruppe im Ziel-Netz. Das Eingabefeld "Quell-Umsetzung" ist deshalb nicht projektierbar.
Ziel-IP-Adresse	IP-Adresse im Quell-Netz	Ziel-IP-Adresse im Quell-Netz, über die auf eine IP-Adresse im Ziel-Netz zugegriffen werden soll. Stimmt in einem Telegramm die Ziel-IP-Adresse mit der eingegebenen IP-Adresse überein, wird die IP-Adresse durch die im Eingabefeld "Ziel-Umsetzung" angegebene IP-Adresse ausgetauscht. Handelt es sich bei der hier eingegebenen IP-Adresse nicht um die IP-Adresse der Security-Baugruppe, wird diese zur Alias-Adresse. Dies bedeutet, dass die angegebene Adresse zusätzlich als IP-Adresse an der ausgewählten Schnittstelle registriert wird. Alias-Adressen werden zusätzlich im Register "Schnittstellen" der Security-Baugruppe angezeigt. Stellen Sie sicher, dass mit der Alias-Adresse kein IP-Adresskonflikt im Netzwerk besteht.
Ziel-Umsetzung	IP-Adresse im Ziel-Netz	Die Ziel-IP-Adresse wird durch die hier angegebene IP-Adresse ersetzt.
Nr.	-	Von SCT vergebene, fortlaufende Nummer, die zur Bezugnahme auf die Firewall-Regel verwendet wird, welche von SCT für die NAT-Regel erzeugt wird.

NAPT aktivieren

Der Eingabebereich für NAPT wird aktiviert. NAPT-Umsetzungen werden erst durch die nachfolgend beschriebenen Einträge in der Liste wirksam. Nach dem Anlegen von NAPT-Regeln werden die zugehörigen Firewall-Regeln erzeugt und im Erweiterten Modus angezeigt, siehe Kapitel:
Zusammenhang zwischen NAT-/NAPT-Router und Firewall (Seite 184)

Die IP-Adressumsetzung mit NAPT kann in folgender Richtung durchgeführt werden:

- Extern nach Intern

Wenn die DMZ-Schnittstelle der Security-Baugruppe (nur SCALANCE S623/S627-2M) aktiviert ist, kann die IP-Adressumsetzung mit NAPT zusätzlich in folgenden Richtungen durchgeführt werden:

- Extern nach DMZ
- DMZ nach Intern
- DMZ nach Extern

Wenn sich die SCALANCE S Baugruppe in einer VPN-Gruppe (nicht für SCALANCE S602) befindet, kann die IP-Adressumsetzung mit NAPT zusätzlich in folgenden Richtungen durchgeführt werden:

- Extern nach Tunnel
- Tunnel nach Intern
- Tunnel nach Extern
- DMZ nach Tunnel (nur bei aktivierter DMZ-Schnittstelle)
- Tunnel nach DMZ (nur bei aktivierter DMZ-Schnittstelle)

Für die Richtung "Extern nach Intern" gilt beispielsweise: Telegramme, die an die externe IP-Adresse der Security-Baugruppe und an den Port gerichtet sind, der in der Spalte "Quell-Port" eingetragen ist, werden an die angegebene Ziel-IP-Adresse im internen Netz sowie an den angegebenen Ziel-Port weitergeleitet.

Die folgende Tabelle zeigt das Eingabeschema für die Adressumsetzung mit NAPT:

Feld	Mögliche Eingaben	Bedeutung
Quell-Port	TCP-/UDP-Port oder -Portbereich Beispiel für die Eingabe eines Portbereiches: 78:99	Ein Teilnehmer im Quell-Netz kann einem Teilnehmer im Ziel-Netz ein Telegramm senden, indem er diese Portnummer verwendet.
Ziel-IP-Adresse	IP-Adresse im Ziel-Netz	Telegramme, die an die IP-Adresse der Security-Baugruppe im Quell-Netz sowie an den im Feld "Quell-Port" angegebenen TCP-/UDP-Port gerichtet sind, werden an die hier angegebene IP-Adresse weitergeleitet.
Ziel-Port	TCP-/UDP-Port	Portnummer, an die die vom Quell-Netz kommenden Telegramme weitergeleitet werden.

Feld	Mögliche Eingaben	Bedeutung
Protokoll	• TCP+UDP • TCP • UDP	Auswahl der Protokollfamilie für die angegebenen Portnummern
Nr.	-	Von SCT vergebene, fortlaufende Nummer, die zur Bezugnahme auf die Firewall-Regel verwendet wird, welche von SCT für die NAPT-Regel erzeugt wird.

Siehe auch

IP-Paketfilter-Regeln (Seite 151)

5.1.5 Adressumsetzung mit NAT/NAPT in VPN-Tunneln



S≥V4.0

Bedeutung

Adressumsetzungen mit NAT/NAPT können auch für Kommunikationsbeziehungen durchgeführt werden, die über VPN-Tunnel aufgebaut sind.

Voraussetzungen

Für eine SCALANCE S Baugruppe, die eine Adressumsetzung mit NAT/NAPT in einem VPN-Tunnel durchführen soll, gelten allgemein die folgenden Voraussetzungen:

- Die SCALANCE S Baugruppe befindet sich in einer VPN-Gruppe.
- Die SCALANCE S Baugruppe befindet sich im Routing-Modus und/oder die DMZ-Schnittstelle der SCALANCE S Baugruppe ist aktiviert.
- Die Tunnel-Schnittstelle ist aktiviert.

Unterstützte Adressumsetzungsrichtungen

Es werden die Adressumsetzungsrichtungen unterstützt, die in folgendem Kapitel beschrieben sind:
Adressumsetzung mit NAT/NAPT (Seite 175)

Unterstützte Adressumsetzungsaktionen

Bei getunnelten Kommunikationsbeziehungen werden die folgenden Adressumsetzungsaktionen unterstützt:

- Destination-NAT ("Redirect")
- Source-NAT ("Masquerading")
- Source- und Destination-NAT ("1:1-NAT")
- NAPT ("Portforwarding")

Grundlegende Informationen zu diesen Adressumsetzungsaktionen finden Sie in folgendem Kapitel:
Adressumsetzung mit NAT/NAPT (Seite 175)

Unterstützte VPN-Kopplungen

Im Zusammenspiel mit NAT/NAPT werden die folgenden VPN-Kopplungen unterstützt:

VPN-Kopplung		VPN-Verbindung wird initiiert von	Adressumsetzung wird durchgeführt von
SCALANCE S (a)	SCALANCE S (b)	SCALANCE S (a) oder SCALANCE S (b)	SCALANCE S (a) und/oder SCALANCE S (b)
SCALANCE S	S7-CP / PC-CP	SCALANCE S oder S7-CP / PC-CP	SCALANCE S
SCALANCE S	SCALANCE M	SCALANCE M	SCALANCE S und/oder SCALANCE M*
SOFTNET Security Client	SCALANCE S	SOFTNET Security Client	SCALANCE S
SCALANCE S	NCP VPN-Client (Android)	NCP VPN-Client (Android)	SCALANCE S

* Es wird ausschließlich 1:1-NAT unterstützt.

SCALANCE S Baugruppen vom Typ SCALANCE S623 V4 und SCALANCE S627-2M V4, die einen VPN-Endpunkt an der externen Schnittstelle und an der DMZ-Schnittstelle besitzen, können an beiden Schnittstellen gleichzeitig Adressumsetzungen durchführen.

Adressumsetzungsverhalten bei Teilnahme an mehreren VPN-Gruppen

Ist eine SCALANCE S Baugruppe Teilnehmer mehrerer VPN-Gruppen, dann gelten die Adressumsetzungsregeln, die für die Tunnel-Schnittstelle der SCALANCE S Baugruppe projektiert wurden, für alle VPN-Verbindungen dieser SCALANCE S Baugruppe.

Beachten Sie:

Sobald Sie eine NAT-Adressumsetzung in oder aus Richtung Tunnel konfiguriert haben, sind lediglich noch die beteiligten IP-Adressen der NAT-Adressumsetzungsregeln über den VPN-Tunnel erreichbar.

5.1.6 Zusammenhang zwischen NAT-/NAPT-Router und Firewall

Bedeutung

Von SCT werden nach dem Anlegen von NAT-/NAPT-Regeln automatisch Firewall-Regeln erzeugt, die die Kommunikation in der projektierten Adressumsetzungsrichtung freigeben. Die erzeugten Firewall-Regeln können ggf. erweitert werden (zusätzliche IP-Adressen / IP-Adressbereich / IP-Adressband, Dienste, Bandbreite). Zudem sollten die automatisch erzeugten Firewall-Regeln im Hinblick auf ihre Priorität bezüglich ihrer Position überprüft werden. Befinden sich zusätzlich manuell projektierte Firewall-Regeln in der Regelliste, die höher priorisiert sind als die automatisch erzeugten Firewall-Regeln, wird unter Umständen kein NAT/NAPT durchgeführt.

Von SCT erzeugte Firewall-Parameter können nicht angepasst werden. Nach dem Deaktivieren von NAT/NAPT werden die von SCT erzeugten Firewall-Regeln entfernt.

Zur einfacheren Bezugnahme zwischen NAT-/NAPT-Regeln und den zugehörigen Firewall-Regeln sind die Regeln in den Registern "NAT/NAPT" und "Firewall" mit korrespondierenden, fortlaufenden Nummern gekennzeichnet.

In der folgenden Tabelle werden die Schemata der Firewall-Regeln dargestellt, die für SCALANCE S Baugruppen für NAT-Regeln erzeugt werden.

Tabelle 5- 1 NAT-Adressumsetzung und zugehörige Firewall-Regeln für SCALANCE S Baugruppen

NAT-Aktion	Angelegte Firewall-Regel				
	Aktion	**Von**	**Nach**	**Quell-IP-Adresse**	**Ziel-IP-Adresse**
Destination-NAT	Allow	Quell-Netz	Ziel-Netz	-	IP-Adresse, die im Eingabefeld "Ziel-IP-Adresse" angegeben wurde
Source-NAT	Allow	Quell-Netz	Ziel-Netz	IP-Adresse des Teilnehmers, die im Eingabefeld "Quell-IP-Adresse" angegeben wurde	-
Source-NAT + Destination-NAT	Allow	Quell-Netz	Ziel-Netz	IP-Adresse des Teilnehmers, die im Eingabefeld "Quell-IP-Adresse" angegeben wurde	-
	Allow	Ziel-Netz	Quell-Netz	-	IP-Adresse, die von SCT in das Eingabefeld "Ziel-IP-Adresse" eingefügt wurde

NAT-Aktion	Angelegte Firewall-Regel				
	Aktion	**Von**	**Nach**	**Quell-IP-Adresse**	**Ziel-IP-Adresse**
Double-NAT	Allow	Quell-Netz	Ziel-Netz	IP-Adresse des Teilnehmers, die im Eingabefeld "Quell-IP-Adresse" angegeben wurde	IP-Adresse, die im Eingabefeld "Ziel-IP-Adresse" angegeben wurde
	Allow	Quell-Netz	Ziel-Netz	IP-Adresse des Teilnehmers, die im Eingabefeld "Quell-IP-Adresse" angegeben wurde	IP-Adresse des Teilnehmers, die im Eingabefeld "Ziel-Umsetzung" angegeben wurde

In der folgenden Tabelle werden die Schemata der Firewall-Regeln dargestellt, die für CP x43-1 Adv. für NAT-Regeln erzeugt werden.

Tabelle 5- 2 NAT-Adressumsetzung und zugehörige Firewall-Regeln für CP x43-1 Adv.

NAT-Aktion	Angelegte Firewall-Regel				
	Aktion	**Von**	**Nach**	**Quell-IP-Adresse**	**Ziel-IP-Adresse**
Destination-NAT	Drop	Extern	Station	-	-
	Allow	Extern	Any	-	IP-Adresse des Teilnehmers, die im Eingabefeld "Ziel-Umsetzung" angegeben wurde
Source-NAT	Allow	Any	Extern	IP-Adresse, die im Eingabefeld "Quell-Umsetzung" angegeben wurde	-
Source-NAT + Destination-NAT	Allow	Any	Extern	IP-Adresse, die im Eingabefeld "Quell-Umsetzung" angegeben wurde	-
	Drop	Extern	Station	-	-
	Allow	Extern	Any	-	IP-Adresse des Teilnehmers, die im Eingabefeld "Ziel-Umsetzung" angegeben wurde

In der folgenden Tabelle wird das Schema für Firewall-Regeln dargestellt, die für SCALANCE S Baugruppen für NAPT-Regeln erzeugt werden.

Tabelle 5- 3 NAPT-Umsetzungen und angelegte Firewall-Regeln für SCALANCE S Baugruppen

Angelegte Firewall-Regel					
Aktion	**Von**	**Nach**	**Quell-IP-Adresse**	**Ziel-IP-Adresse**	**Dienst**
Allow	Quell-Netz	Ziel-Netz	-	IP-Adresse der Security-Baugruppe im Quell-Netz	[Dienst_NAPT-Regel]

In der folgenden Tabelle wird das Schema für Firewall-Regeln dargestellt, die für CP x43-1 Adv. für NAPT-Regeln erzeugt werden.

Tabelle 5- 4 NAPT-Umsetzungen und angelegte Firewall-Regeln für CP x43-1 Adv.

Angelegte Firewall-Regeln					
Aktion	**Von**	**Nach**	**Quell-IP-Adresse**	**Ziel-IP-Adresse**	**Dienst**
Drop	Extern	Station	-	-	[Dienst_NAPT-Regel]
Allow	Extern	Any	-	IP-Adresse des Teilnehmers, die im Eingabefeld "Ziel-IP-Adresse" angegeben wurde	[Dienst_NAPT-Regel]

Stateful Packet Inspection

Firewall und NAT-/NAPT-Router unterstützen den Mechanismus "Stateful Packet Inspection". Daher können Antworttelegramme den NAT-/NAPT-Router und die Firewall passieren, ohne dass deren Adressen in der Firewall-Regel und der NAT/NAPT-Adressumsetzung zusätzlich aufgenommen werden müssen.

5.1.7 Zusammenhang zwischen NAT-/NAPT-Router und benutzerspezifischer Firewall

Bedeutung

Von SCT wird nach dem Anlegen von NAT-/NAPT-Regeln in der benutzerspezifischen Firewall automatisch ein benutzerspezifischer IP-Regelsatz erzeugt, der die Kommunikation in der projektierten Adressumsetzungsrichtung freigibt. Diesen benutzerspezifischen IP-Regelsatz können Sie dann einzelnen oder mehreren Benutzern und/oder einzelnen oder mehreren Rollen (nur für SCALANCE S Baugruppen ab V4) zuweisen.

Die erzeugten Firewall-Regeln können ggf. verschoben und erweitert werden (zusätzliche IP-Adresse, Dienste, Bandbreite). Von SCT erzeugte Firewall-Parameter können nicht angepasst werden. Wird der benutzerspezifische IP-Regelsatz auf eine Security-Baugruppe mit deaktiviertem NAT/NAPT per Drag and Drop gezogen, dann kommen die NAT-/NAPT-Regeln aus der benutzerspezifischen Firewall ebenso auf dieser Security-Baugruppe nicht zur Anwendung.

Hinweis

Die Adressumsetzungsaktion "Double-NAT" wird in Zusammenhang mit der benutzerspezifischen Firewall nicht unterstützt.

So erreichen Sie diese Funktion

Register "NAT" bzw. "NAPT" im Konfigurationsdialog für benutzerspezifische IP-Regelsätze, siehe folgendes Kapitel:
Benutzerspezifische IP-Regelsätze (Seite 143)

Unterstützte Adressumsetzungsrichtungen für die Aktion "Source-NAT"

Die Aktion "Source-NAT" kann in folgenden Richtungen durchgeführt werden.

- Extern nach DMZ
- DMZ nach Extern

Im Feld "Quell-IP-Adresse" kann keine IP-Adresse eingetragen werden. Diese wird bei der Anmeldung des Teilnehmers an der Security-Baugruppe automatisch eingetragen.

Unterstützte Adressumsetzungsrichtungen für die Aktion "Destination-NAT"

Die Aktion "Destination-NAT" kann in folgenden Richtungen durchgeführt werden:

- Extern nach Intern
- Extern nach DMZ
- DMZ nach Intern
- DMZ nach Extern
- Tunnel nach Intern (nur SCALANCE S612/S623/S627-2M ab V4)
- Tunnel nach Extern (nur SCALANCE S612/S623/S627-2M ab V4)
- Tunnel nach DMZ (nur SCALANCE S612/S623/S627-2M ab V4)

Unterstützte Adressumsetzungsrichtungen für die Aktion "Source-NAT + Destination-NAT"

Die Aktion "Source-NAT + Destination-NAT" kann in folgenden Richtungen durchgeführt werden:

- Extern nach DMZ
- DMZ nach Extern

Im Feld "Quell-IP-Adresse" kann keine IP-Adresse eingetragen werden. Diese wird bei der Anmeldung des Teilnehmers an der Security-Baugruppe automatisch eingetragen.

Unterstützte Adressumsetzungsrichtungen für NAPT

Die Adressumsetzung mit NAPT kann in folgenden Richtungen durchgeführt werden:

- Extern nach Intern
- Extern nach DMZ
- DMZ nach Intern
- DMZ nach Extern
- Tunnel nach Intern (nur SCALANCE S612/S623/S627-2M ab V4)
- Tunnel nach Extern (nur SCALANCE S612/S623/S627-2M ab V4)
- Tunnel nach DMZ (nur SCALANCE S612/S623/S627-2M ab V4)

NAT-/NAPT-Adressumsetzung und zugehörige benutzerspezifische IP-Regelsätze

In den Firewall-Regeln für benutzerspezifische IP-Regelsätze, die auf Basis von NAT-/NAPT-Regeln erzeugt werden, kann im Feld "Quell-IP-Adresse" keine IP-Adresse eingetragen werden. Diese wird bei der Anmeldung des Teilnehmers am Security-Modul automatisch eingetragen. Die restlichen Eigenschaften sind zu den Firewall-Regeln, die lokal für einzelne Security-Module erzeugt werden, identisch. Siehe Kapitel:
Zusammenhang zwischen NAT-/NAPT-Router und Firewall (Seite 184)

5.2 Security-Baugruppe als DHCP-Server

5.2.1 Übersicht



Übersicht

Sie können die Security-Baugruppe am internen Netz und am DMZ-Netz als DHCP-Server (DHCP = Dynamic Host Configuration Protokoll) betreiben. Damit ist es möglich, den angeschlossenen Geräten automatisch IP-Adressen zuzuweisen.

Der gleichzeitige DHCP-Server-Betrieb an beiden Schnittstellen ist möglich. S62x

Die IP-Adressen werden entweder dynamisch aus einem von Ihnen vergebenen Adressband verteilt oder es wird gemäß Ihrer Vorgabe eine bestimmte IP-Adresse einem bestimmten Gerät zugewiesen. Sollen Geräte an der internen Schnittstelle bzw. an der DMZ-Schnittstelle für die Firewall-Konfiguration immer die gleiche IP-Adresse bekommen, darf die Adresszuordnung nur statisch anhand der MAC-Adresse oder anhand der Client-ID erfolgen.

Voraussetzung

Sie müssen die Geräte im internen Netz bzw. im DMZ-Netz so konfigurieren, dass diese die IP-Adresse von einem DHCP-Server beziehen.

Je nach Betriebsart übermittelt die Security-Baugruppe den Teilnehmern im jeweiligen Subnetz eine IP-Adresse des Standard-Routers oder Sie müssen den Teilnehmern im Subnetz eine Router-IP-Adresse bekannt machen.

- Router-IP-Adresse wird übermittelt

  In folgenden Fällen wird durch das DHCP-Protokoll von der Security-Baugruppe eine Router-IP-Adresse an den Teilnehmer übermittelt:

  – Der Teilnehmer befindet sich an der DMZ-Schnittstelle (nur SCALANCE S623/S627-2M)
  Die Security-Baugruppe übermittelt in diesem Fall die eigene IP-Adresse als Router-IP-Adresse.

  – Der Teilnehmer befindet sich an der internen Schnittstelle und die Security-Baugruppe ist für den Router-Betrieb konfiguriert
  Die Security-Baugruppe übermittelt in diesem Fall die eigene IP-Adresse als Router-IP-Adresse.

  – Der Teilnehmer befindet sich an der internen Schnittstelle und die Security-Baugruppe ist nicht für den Router-Betrieb konfiguriert, es ist aber in der Konfiguration der Security-Baugruppe ein Standard-Router angegeben.
  Die Security-Baugruppe übermittelt in diesem Fall die IP-Adresse des Standard-Routers als Router-IP-Adresse.

- Router-IP-Adresse wird nicht übermittelt

  Tragen Sie in folgenden Fällen die Router-IP-Adresse beim Teilnehmer manuell ein:

  – Der Teilnehmer befindet sich an der internen Schnittstelle und die Security-Baugruppe ist nicht für den Router-Betrieb konfiguriert. Zusätzlich ist in der Konfiguration der Security-Baugruppe kein Standard-Router angegeben.

Siehe auch

Konsistenzprüfungen (Seite 63)

5.2.2 DHCP-Server konfigurieren

Voraussetzung

Das Register "DHCP-Server" wird nur angezeigt, wenn sich das Projekt im Erweiterten Modus befindet.

Hinweis

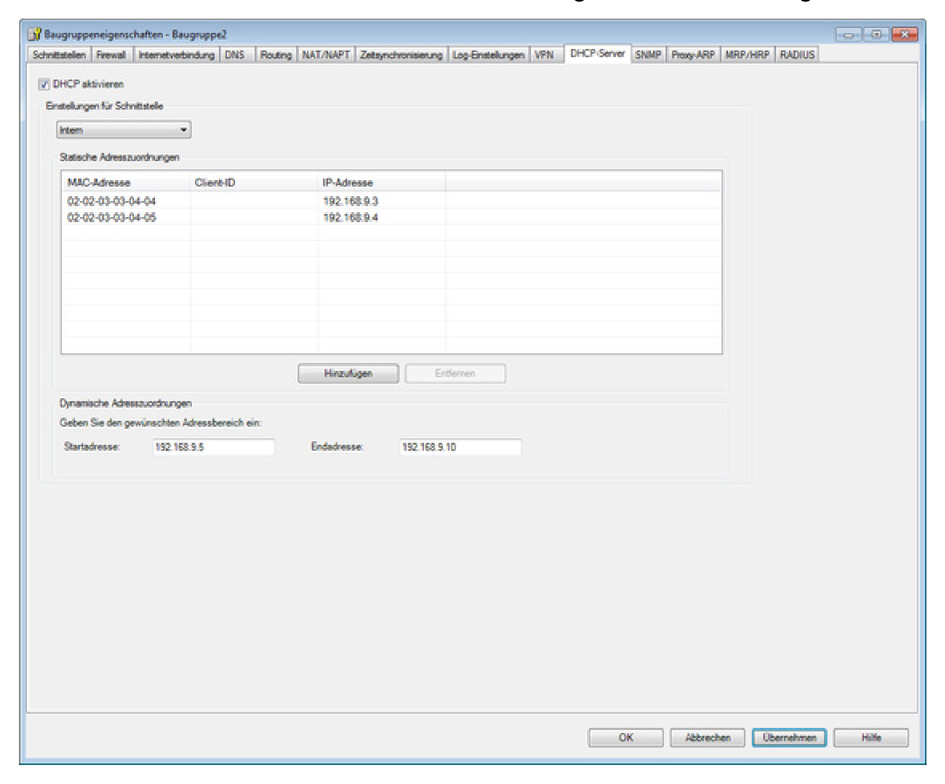
Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.

Abhilfe SCT Standalone: Sie schließen das Projekt ohne zu speichern und öffnen Sie es erneut.

So erreichen Sie diese Funktion

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "DHCP-Server".



3. Aktivieren Sie das Kontrollkästchen "DHCP aktivieren".

4. Wählen Sie aus, für welche Schnittstelle die DHCP-Einstellungen vorgenommen werden sollen.
5. Nehmen Sie die Adresszuordnung vor. Sie haben die beiden folgenden Möglichkeiten zur Konfiguration:

- Statische Adresszuordnungen

  Geräten mit einer bestimmten MAC-Adresse oder Client-ID werden jeweils vorgegebene IP-Adressen zugeordnet. Tragen Sie hierzu diese Geräte in die Adressliste im Eingabebereich "Statische Adresszuordnung" ein. Diese Option ist im Hinblick auf Firewall-Regeln mit expliziter Angabe von Quell- bzw. Ziel-IP-Adresse sinnvoll.

- Dynamische Adresszuordnungen

  Geräte, deren MAC-Adresse oder deren Client-ID nicht explizit angegeben wurde, erhalten eine beliebige IP-Adresse aus dem vorgegebenen Adressband. Dieses Adressband stellen Sie im Eingabebereich "Dynamische Adresszuordnungen" ein.

Hinweis

Dynamische Adressvergabe - Verhalten nach Unterbrechung der Spannungsversorgung

Beachten Sie, dass die dynamisch vergebenen IP-Adressen nicht gespeichert werden, wenn die Spannungsversorgung unterbrochen wird. Nach Wiederkehr der Spannungsversorgung müssen Sie daher dafür sorgen, dass die Teilnehmer erneut eine IP-Adresse anfordern.

Sie sollten daher die dynamische Adressvergabe nur für folgende Teilnehmer vorsehen:

- Teilnehmer, die im Subnetz temporär genutzt werden (wie beispielsweise Service-Geräte);
- Teilnehmer, die eine einmal zugewiesene IP-Adresse bei einer erneuten Anforderung an den DHCP-Server als "Vorzugsadresse" übermitteln (wie beispielsweise PC-Stationen).

Für die Teilnehmer im dauernden Betrieb ist die statische Adresszuweisung über die Angabe einer Client-ID (empfohlen für S7-CPs wegen des einfacheren Baugruppentauschs) oder der MAC-Adresse vorzuziehen.

Symbolische Namen werden unterstützt

Sie können in der hier beschriebenen Funktion die IP- oder MAC-Adressen auch als symbolische Namen eingeben.

Konsistenzprüfung - diese Regeln müssen Sie beachten

Berücksichtigen Sie bei Ihrer Eingabe die nachfolgend aufgeführten Regeln:

- Die in der Adressliste im Eingabebereich "Statische Adresszuordnungen" zugewiesenen IP-Adressen dürfen nicht im Bereich der dynamischen IP-Adressen liegen.
- Symbolische Namen müssen eine numerische Adresszuordnung besitzen. Wenn Sie symbolische Namen hier neu vergeben, müssen Sie noch die Adresszuordnung im Dialog "Symbolische Namen" vornehmen.

- IP-Adressen, MAC-Adressen und Client-IDs dürfen im Eingabebereich "Statische Adresszuordnungen" nur einmal vorkommen (bezogen auf die Security-Baugruppe).
- Sie müssen bei den statisch zugewiesenen IP-Adressen entweder die MAC-Adresse oder die Client-ID (Rechnername) angeben.
- Die Client-ID ist eine Zeichenfolge mit maximal 63 Zeichen. Es dürfen nur die folgenden Zeichen verwendet werden: a-z, A-Z, 0-9 und - (Bindestrich).

  Hinweis

  Bei SIMATIC S7 kann den Geräten an der Ethernet-Schnittstelle für den Bezug einer IP-Adresse über DHCP eine Client-ID zugewiesen werden.

  Bei PCs ist die Vorgehensweise abhängig vom verwendeten Betriebssystem; empfohlen wird, hier die MAC-Adresse für die Zuordnung zu verwenden.
- Sie müssen bei den statisch zugewiesenen IP-Adressen die IP-Adresse angeben.
- Folgende IP-Adressen dürfen nicht im Bereich der dynamischen Adresszuordnungen liegen:
  - alle Router-IP-Adressen im Register "Routing"
  - Syslog-Server
  - Standard-Router
  - Adresse(n) der Security-Baugruppe
- DHCP wird von der Security-Baugruppe an der Schnittstelle zum internen Subnetz und an der Schnittstelle zum DMZ-Netz unterstützt. Aus diesem Betriebsverhalten der Security-Baugruppe ergeben sich weiterhin für IP-Adressen im Bereich der dynamischen Adresszuordnungen folgende Anforderungen:
  - Bridge-Modus

    Der Bereich muss in dem durch die Security-Baugruppe definierten Netz liegen.
  - Routing-Modus

    Der Bereich muss in dem durch die Security-Baugruppe definierten internen Subnetz liegen.

    Hinweis

    Das DMZ-Netz stellt stets ein separates Subnetz dar. Bei Verwendung von DHCP auf der DMZ-Schnittstelle muss beachtet werden, dass sich der freie IP-Adressbereich (dynamische IP-Adressen) innerhalb des DMZ-Subnetzes befindet.
- Der freie IP-Adressbereich muss durch die Angabe der Startadresse und der Endadresse vollständig angegeben sein. Die Endadresse muss größer als die Startadresse sein.
- Die IP-Adressen, die Sie in die Adressliste im Eingabebereich "Statische Adresszuordnungen" eingeben, müssen im Adressbereich des internen Subnetzes bzw. im DMZ-Netz der Security-Baugruppe liegen.

Beachten Sie die Erläuterungen im Kapitel Konsistenzprüfungen (Seite 63).

5.3 Zeitsynchronisierung

5.3.1 Übersicht

Bedeutung

Zur Überprüfung der zeitlichen Gültigkeit eines Zertifikates und für die Zeitstempel von Log-Einträgen wird auf der Security-Baugruppe Datum und Uhrzeit geführt.

Projektierbar sind folgende Alternativen:

- Automatisches Stellen der Baugruppen-Uhrzeit mit der PC-Uhrzeit beim Laden einer Konfiguration. SCA. S
- Automatisches Stellen und periodischer Abgleich der Uhrzeit über einen Network Time Protocol-Server (NTP-Server).

Hinweis

Bevor die Security-Funktionen eines CPs zur Anwendung kommen, muss dieser ein gültiges Uhrzeitsynchronisationstelegramm vom Uhrzeit-Master erhalten.

Synchronisierung durch einen NTP-Server

Beim Anlegen des NTP-Servers gelten die folgenden Regeln:

- NTP-Server können über das SCT-Menü "Optionen" > "Konfiguration der NTP-Server..." projektweit angelegt werden. Weisen Sie einen NTP-Server über das Eigenschaften-Register "Zeitsynchronisierung" einer Security-Baugruppe zu. Verwenden verschiedene Security-Baugruppen im SCT-Projekt denselben NTP-Server, so müssen dessen Daten nur einmal eingegeben werden.
- Sie können projektweit 32 NTP-Server anlegen.
- Sie können einer Security-Baugruppe max. 4 NTP-Server zuweisen.
- Symbolische Namen werden bei der Definition von NTP-Servern unterstützt.
- FQDNs werden bei der Definition von NTP-Servern unterstützt.
- Von bereits in STEP 7 angelegten NTP-Servern wird die IP-Adresse und das Aktualisierungsintervall nach SCT migriert. CP
- Bei Auswahl von "Zeitsynchronisation mit NTP (gesichert)" akzeptiert die Security-Baugruppe nur die Zeit von entsprechend konfigurierten gesicherten NTP-Servern (gesichert). Eine gemischte Konfiguration von ungesicherten und gesicherten NTP-Servern (gesichert) auf einer Security-Baugruppe ist nicht möglich.

5.3.2 Uhrzeitführung konfigurieren

So erreichen Sie diese Funktion

Menübefehl SCT:

1. Selektieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Zeitsynchronisierung".

Menübefehl STEP 7 (wenn die Option "Uhrzeitsynchronisation im NTP Verfahren einschalten" aktiviert ist): "Uhrzeitsynchronisation" > "Erweiterte NTP-Konfiguration aktivieren", Schaltfläche "Ausführen".

Alternativen der Zeitsynchronisierung

Projektierbar sind folgende Alternativen:

Tabelle 5- 5 Zeitsynchronisierung für CP

Auswahlmöglichkeit	Bedeutung / Auswirkung
Keine Zeitsynchronisation	Keine Zeitsynchronisation über den PC oder einen NTP-Server.
Zeitsynchronisation mit NTP	Automatisches Stellen und periodischer Abgleich der Uhrzeit mittels eines NTP-Servers.
Zeitsynchronisation mit NTP (gesichert)	Automatisches Stellen und periodischer Abgleich der Uhrzeit mittels eines NTP-Servers (gesichert).

Tabelle 5- 6 Zeitsynchronisierung für SCALANCE S ≥ V3.0

Auswahlmöglichkeit	Bedeutung / Auswirkung
Keine Zeitsynchronisation	Keine Zeitsynchronisation.
Zeit bei jedem Laden setzen	Automatisches Stellen der Baugruppen-Uhrzeit mit der PC-Uhrzeit beim Laden einer Konfiguration.
Zeitsynchronisation mit NTP	Automatisches Stellen der Uhrzeit mittels eines NTP-Servers.
Zeitsynchronisation mit NTP (gesichert) S≥V4.0	Automatisches Stellen und periodischer Abgleich der Uhrzeit mittels eines NTP-Servers (gesichert).

Modus zur Zeitsynchronisierung auswählen

Gehen Sie folgendermaßen vor:

1. Wählen Sie den Synchronisierungsmodus aus.
2. Für SCALANCE S < V3.0: Bei der Synchronisierung durch einen NTP-Server geben Sie das Aktualisierungsintervall in Sekunden ein. Für SCALANCE S ≥ V3.0 wird das Zeitintervall für die Abfrage des NTP-Servers automatisch festgelegt.

Hinweis



In STEP 7 angelegte NTP-Server werden automatisch mit dem Aktualisierungsintervall nach SCT migriert. Das Aktualisierungsintervall kann nur in STEP 7 geändert werden.

---

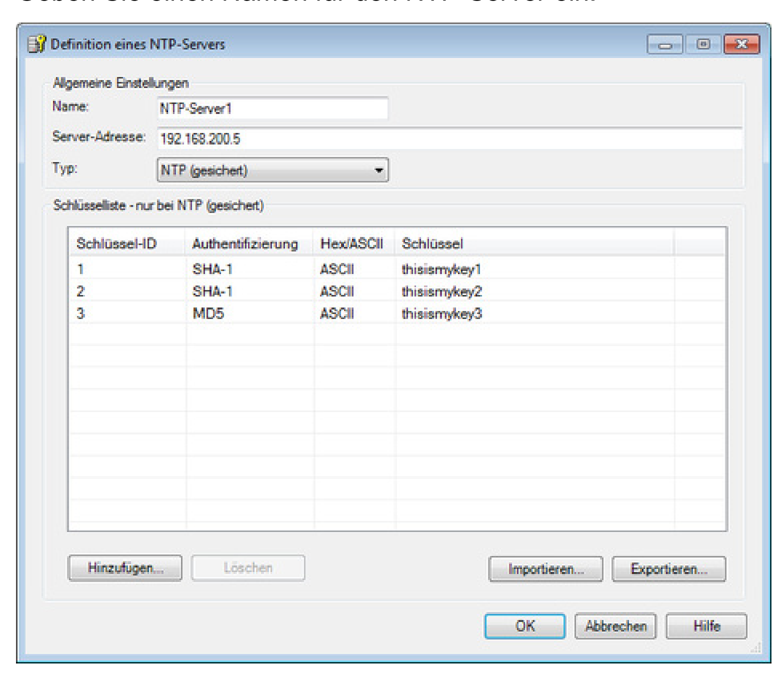
3. Wenn Sie den Synchronisierungsmodus "Zeitsynchronisation mit NTP" bzw. "Zeitsynchronisation mit NTP (gesichert)" ausgewählt haben, weisen Sie der Security-Baugruppe über die Schaltfläche "Hinzufügen" einen bereits angelegten NTP-Server vom selben Typ zu, wie im Feld "Synchronisierungsmodus" ausgewählt.

   Sind noch keine NTP-Server vorhanden, legen Sie über die Schaltfläche "Server konfigurieren..." einen NTP-Server an.

5.3.3 NTP-Server definieren

So definieren Sie einen neuen NTP-Server:

1. Geben Sie einen Namen für den NTP-Server ein.



2. Geben Sie die IP-Adresse / den FQDN des NTP-Servers ein.
3. Wählen Sie den Typ aus.

Einstellungen für NTP (gesichert)

1. Klicken Sie auf die Schaltfläche "Hinzufügen...".
2. Geben Sie die folgenden Daten ein:

Parameter	Bedeutung
Schlüssel-ID	Numerischer Wert zwischen 1 ... 65534.
Authentifizierung	Wählen Sie den Authentifizierungsalgorithmus aus.
Hex/ASCII	Wählen Sie das Format für den NTP-Schlüssel aus.
Schlüssel	Geben Sie den NTP-Schlüssel mit folgenden Längen ein: Hex: 22 ... 40 Zeichen ASCII: 11 ... 20 Zeichen

Import / Export von NTP-Servern

Über die Schaltflächen "Importieren..." bzw. "Exportieren..." können Sie die Schlüsselliste des aktuell angezeigten NTP-Servers exportieren und die Datei in einen NTP-Server importieren bzw. umgekehrt.

5.4 SNMP

5.4.1 Übersicht

Was ist SNMP?

Die Security-Baugruppe unterstützt die Übertragung von Managementinformationen über das Simple Network Management Protocol (SNMP). Dafür ist auf der Security-Baugruppe ein "SNMP-Agent" installiert, der die SNMP-Anfragen entgegennimmt und beantwortet. Informationen über die Eigenschaften von SNMP-fähigen Geräten sind in sogenannten MIB-Dateien (Management Information Base) hinterlegt, für die der Benutzer die notwendigen Rechte (SNMPv3) haben muss.

Bei SNMPv1 wird der "Community String" mitgesendet. Der "Community String" ist wie ein Passwort, welches zusammen mit der SNMP-Anfrage verschickt wird. Ist der Community String korrekt, antwortet die Security-Baugruppe mit der angeforderten Information. Ist der String falsch, verwirft die Security-Baugruppe die Anfrage und antwortet nicht.

Bei SNMPv3 können die Daten verschlüsselt übertragen werden.

5.4.2 SNMP aktivieren



Voraussetzung

HW Konfig: In den CP-Eigenschaften ist im Register "SNMP" das Kontrollkästchen "SNMP aktivieren" aktiviert. Ist es nicht aktiviert, kann SNMP im Security Configuration Tool nicht konfiguriert werden. CP

SNMP konfigurieren - Gehen Sie so vor:

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "SNMP".
3. Aktivieren Sie das Kontrollkästchen "SNMP aktivieren". SCA. S

4. Wählen Sie eine der SNMP-Protokollversionen aus.

Hinweis

Verschlüsselte Datenübertragung bei SNMPv3

Um die Sicherheit zu erhöhen, sollten Sie SNMPv3 verwenden, da die Daten hierbei verschlüsselt übertragen werden.

   – SNMPv1

     Die Security-Baugruppe verwendet zur Steuerung der Zugriffsrechte im SNMP-Agent folgende Standardwerte für die Community Strings:

     Für Lesezugriff: public

     Für Lese- und Schreibzugriff: private

     Um den Schreibzugriff über SNMP zu aktivieren, aktivieren Sie das Optionskästchen "Erlaube schreibenden Zugriff".

   – SNMPv3

     Wählen Sie entweder ein Authentifizierungsverfahren oder ein Authentifizierungs- und Verschlüsselungsverfahren aus.

     Authentifizierungsalgorithmus: keine, MD5, SHA-1

     Verschlüsselungsalgorithmus: keine, AES-128, DES

Hinweis

Verwendung von DES vermeiden

Bei DES handelt es sich um einen unsicheren Verschlüsselungsalgorithmus. Er sollte deshalb nur aus Gründen der Abwärtskompatibilität verwendet werden.

Hinweis

Bei der Verwendung von SNMPv3 ist keine RADIUS-Authentifizierung möglich.

5. Konfigurieren Sie im Bereich "Erweiterte Einstellungen" baugruppenspezifische Angaben zu Autor, Ort und E-Mail-Adresse, welche die Angaben aus den Projekteigenschaften überschreiben.
   Wenn Sie das Kontrollkästchen "Durch SNMP-Set geschriebene Werte beibehalten" aktivieren, werden Werte, die durch ein SNMP-Werkzeug über einen SNMP-SET-Befehl auf die Security-Baugruppe geschrieben wurden, durch das erneute Laden einer SCT-Konfiguration auf die Security-Baugruppe nicht überschrieben. SCA. S

6. Wenn SNMPv3 verwendet werden soll, weisen Sie einem Benutzer eine Rolle zu, bei der die entsprechenden SNMP-Rechte aktiviert sind, damit er die Security-Baugruppe über SNMP erreichen kann.

   Für nähere Informationen zur Konfiguration von Benutzern, Rechten und Rollen, siehe folgendes Kapitel:

   – Benutzer verwalten (Seite 67)

5.5 Proxy-ARP



Übersicht

Proxy-ARP ermöglicht Routern, ARP-Anfragen für Hosts zu beantworten. Die Hosts befinden sich dabei in durch Router getrennten Netzen, verwenden jedoch den gleichen IP-Adressenbereich.

Sendet PC1 eine ARP-Anforderung an PC2, bekommt er von der dazwischen liegenden Security-Baugruppe und nicht von PC2 eine ARP-Antwort und die Hardwareadresse der Schnittstelle (MAC-Adresse des Ports der Security-Baugruppe), auf der die Anfrage empfangen wurde. Der anfragende PC1 sendet dann seine Daten an die Security-Baugruppe, die sie dann an PC2 weiterleitet.

So erreichen Sie diese Funktion

Diese Funktion ist nur für die interne Schnittstelle einer Security-Baugruppe verfügbar, die Teilnehmer einer VPN-Gruppe ist und sich im Bridge-Modus befindet. Zusätzlich muss sich das Projekt im Erweiterten Modus befinden.

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Proxy-ARP".
3. Wenn die Security-Baugruppe eine ARP-Anfrage aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantworten soll, tragen Sie die entsprechende IP-Adresse ein.

Gesicherte Kommunikation im VPN über IPsec-Tunnel 6



In diesem Kapitel erfahren Sie, wie Sie die von der Security- bzw. SCALANCE M Baugruppe geschützten IP-Subnetze zu einem VPN (Virtual Private Network) verbinden.

Wie bereits im Kapitel zu den Baugruppeneigenschaften beschrieben, können Sie es auch hier bei Standard-Einstellungen belassen, um eine sichere Kommunikation Ihrer internen Netze zu gewährleisten.

Weitere Informationen



Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

Siehe auch

Online-Funktionen - Diagnose und Logging (Seite 257)

6.1 VPN mit Security- und SCALANCE M Baugruppen

Sichere Verbindung durch ungeschütztes Netz

Für Security- und SCALANCE M Baugruppen, die das interne Netz schützen, stellen IPsec-Tunnel eine gesicherte Datenverbindung durch das unsichere externe Netz zur Verfügung.

Durch den Datenaustausch über IPsec werden für die Kommunikation die folgenden Sicherheitsaspekte realisiert:

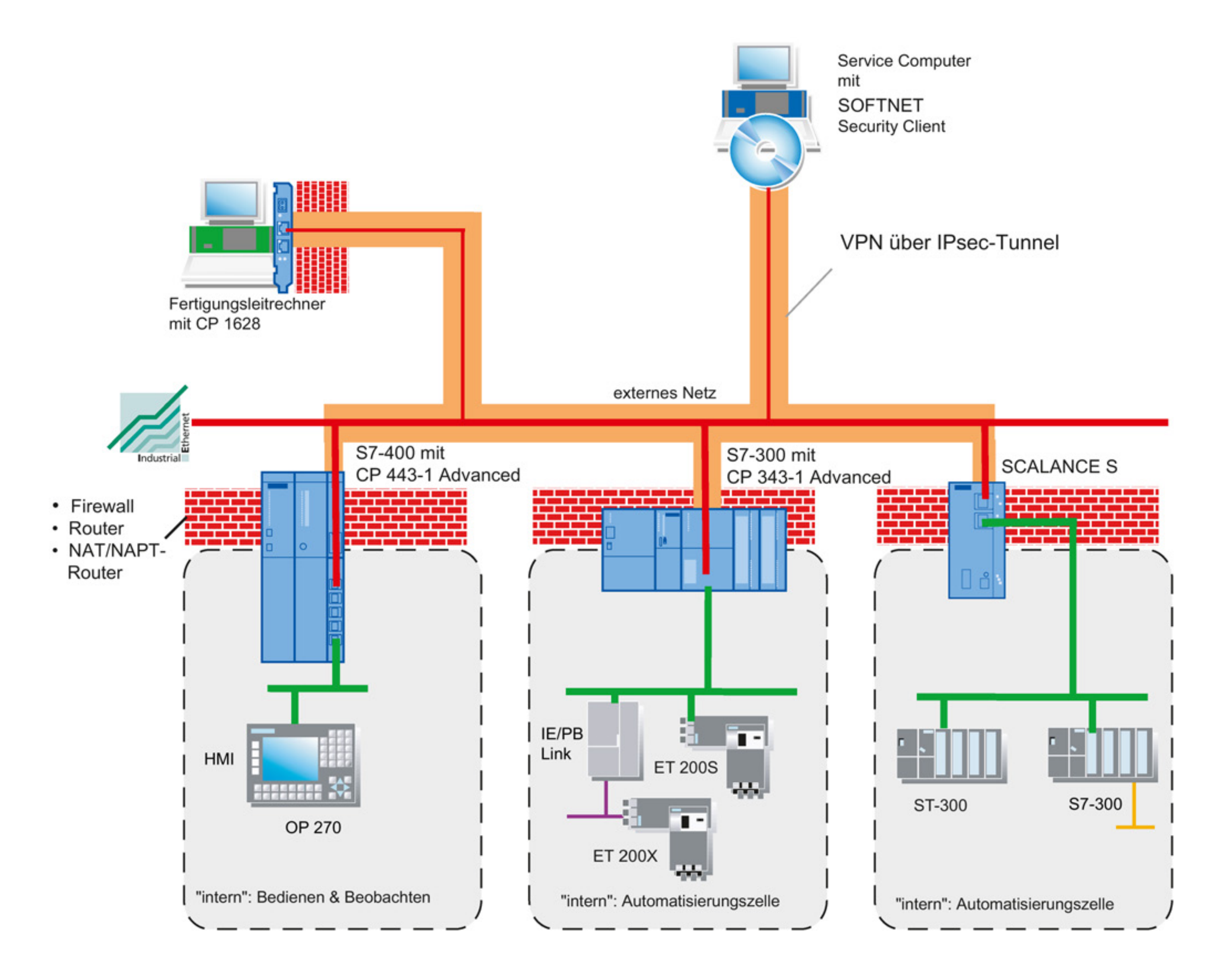
- Vertraulichkeit

  Stellt sicher, dass die Daten verschlüsselt übertragen werden.
- Integrität

  Stellt sicher, dass die Daten nicht verändert worden sind.
- Authentizität

  Stellt sicher, dass die VPN-Endpunkte auch vertrauenswürdig sind.

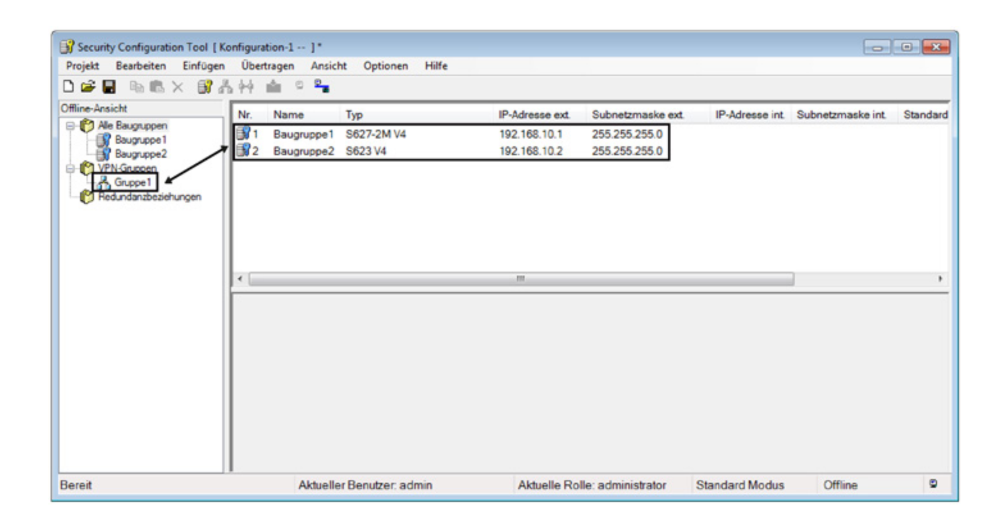
Die Baugruppe verwendet für die Tunnelung das IPsec-Protokoll (Tunnelmodus von IPsec).



Tunnelverbindungen bestehen zwischen Baugruppen der gleichen VPN-Gruppe

Die Eigenschaften eines VPN werden bei den Baugruppen innerhalb einer VPN-Gruppe für alle IPsec-Tunnel zusammengefasst.

IPsec-Tunnel werden automatisch zwischen allen Baugruppen und SOFTNET Security Clients aufgebaut, die einer VPN-Gruppe angehören. Dabei kann eine Baugruppe in einem Projekt parallel mehreren verschiedenen VPN-Gruppen angehören.



Hinweis

Wird der Name einer Baugruppe geändert, dann müssen alle Baugruppen derjenigen VPN-Gruppen, denen die geänderte Baugruppe angehört, neu konfiguriert werden (Menübefehl "Übertragen" > "An alle Baugruppen...").

Wird der Name einer VPN-Gruppe geändert, dann müssen alle Baugruppen dieser VPN-Gruppe neu konfiguriert werden (Menübefehl "Übertragen" > "An alle Baugruppen...").

Hinweis

Layer-2-Telegramme werden auch getunnelt, wenn sich zwischen zwei Baugruppen ein Router befindet. Dazu müssen jedoch die MAC-Adressen der Kommunikationspartner statisch im Security Configuration Tool konfiguriert werden und gegebenenfalls statische ARP-Einträge auf den Kommunikationsgeräten eingetragen werden.

Allgemein gilt: Non-IP-Telegramme werden nur dann durch einen Tunnel übertragen, wenn die Geräte, die die Telegramme senden bzw. empfangen, auch schon vorher, d. h. ohne den Einsatz der Baugruppen, kommunizieren konnten.

6.2 Authentifizierungsverfahren

Authentifizierungsverfahren

Das Authentifizierungsverfahren wird innerhalb einer VPN-Gruppe festgelegt und bestimmt die Art der verwendeten Authentifizierung.

Es werden schlüsselbasierende oder zertifikatsbasierende Authentifizierungsverfahren unterstützt:

- Preshared Keys

  Die Authentifizierung erfolgt über eine zuvor verabredete Zeichenfolge, die an alle in der VPN-Gruppe befindlichen Baugruppen verteilt wird.

  Geben Sie dafür im Dialog "VPN-Gruppeneigenschaften" im Feld "Schlüssel" ein Passwort ein oder erzeugen Sie ein Passwort über die Schaltfläche "Neu...".

- Zertifikat

  Die zertifikatbasierte Authentifizierung "Zertifikat" ist die Standardeinstellung, die auch im Standard Modus eingeschaltet ist. Das Verhalten ist wie folgt:

  – Beim Anlegen einer VPN-Gruppe wird automatisch ein CA-Zertifikat für die VPN-Gruppe erzeugt.

  – Jede Baugruppe, die in der VPN-Gruppe ist, erhält ein VPN-Gruppen-Zertifikat, das mit dem Schlüssel der Zertifizierungsstelle der VPN-Gruppe signiert ist.

  Sämtliche Zertifikate basieren auf dem ITU-Standard X.509v3 (ITU, International Telecommunications Union).

  Die Zertifikate werden von einer im Security Configuration Tool enthaltenen Zertifizierungsstelle erzeugt.

Hinweis

Einschränkung bei VLAN-Betrieb

Bei IP-Telegrammen durch den VPN-Tunnel der Baugruppe wird kein VLAN-Tagging übertragen. Die in den IP-Telegrammen enthaltenen VLAN-Tags gehen beim Passieren der Baugruppen verloren, da für die Übertragung der IP-Telegramme IPsec verwendet wird.

Standardmäßig können mit IPsec keine IP-Broadcast- bzw. IP-Multicast-Telegramme durch einen Layer 3 VPN-Tunnel übertragen werden. Durch einen Layer 2 VPN-Tunnel der Security-Baugruppe werden IP-Broadcast- bzw. IP-Multicast-Telegramme genau wie MAC-Pakete inklusive Ethernet-Header in UDP "verpackt" und übertragen. Daher bleibt bei diesen Paketen das VLAN-Tagging erhalten.

6.3 VPN-Gruppen

6.3.1 Regeln für die Bildung von VPN-Gruppen

Beachten Sie die folgenden Regeln:

- Für SCALANCE S612 / S613 / S623 / S627-2M / SCALANCE M / VPN-Gerät

  Die erste einer VPN-Gruppe zugeordnete Baugruppe bestimmt, welche zusätzlichen Baugruppen hinzugefügt werden können.

  Ist die erste hinzugefügte SCALANCE S Baugruppe im Routing-Modus oder handelt es sich bei der ersten Baugruppe um eine SCALANCE M Baugruppe bzw. um ein VPN-Gerät, so können zusätzlich nur SCALANCE S Baugruppen mit aktiviertem Routing oder SCALANCE M Baugruppen bzw. VPN-Geräte hinzugefügt werden, da SCALANCE M Baugruppen sowie VPN-Geräte immer im Routing-Modus betrieben werden.
  Ist die erste hinzugefügte SCALANCE S Baugruppe im Bridge-Modus, so können zusätzlich nur SCALANCE S Baugruppen im Bridge-Modus hinzugefügt werden.
  Ein CP, ein SSC sowie ein NCP VPN-Client (Android) kann einer VPN-Gruppe mit einem SCALANCE S im Bridge- oder Routing-Modus hinzugefügt werden.

- Für CP / SSC / NCP VPN-Client (Android)

  Befindet sich ein CP / SSC / NCP VPN-Client (Android) als erstes in einer VPN-Gruppe, dann können Baugruppen in beliebigen Modi hinzugefügt werden, bis eine SCALANCE S oder SCALANCE M Baugruppe hinzugefügt wird. Ab diesem Zeitpunkt gelten die Regeln für SCALANCE S und SCALANCE M Baugruppen, siehe oben.

- Es ist nicht möglich, eine SCALANCE M Baugruppe einer VPN-Gruppe hinzuzufügen, die eine SCALANCE S Baugruppe im Bridge-Modus enthält.

Entnehmen Sie der folgenden Tabelle, welche Baugruppen in einer VPN-Gruppe zusammengefasst werden können:

Tabelle 6- 1 Regeln für die Bildung von VPN-Gruppen

Baugruppe	Kann aufgenommen werden in VPN-Gruppe mit folgender enthaltener Baugruppe:		
	SCALANCE S im Bridge-Modus	SCALANCE S im Routing-Modus / SCALANCE M / VPN-Gerät / NCP VPN-Client (Android)	CP / SSC
SCALANCE S im Bridge-Modus	x	-	x
SCALANCE S im Routing-Modus	-	x	x
CP x43-1 Adv.	x	x	x
CP 1628	x	x	x
SOFTNET Security Client 2005	x	-	-

Baugruppe	Kann aufgenommen werden in VPN-Gruppe mit folgender enthaltener Baugruppe:		
	SCALANCE S im Bridge-Modus	SCALANCE S im Routing-Modus / SCALANCE M / VPN-Gerät / NCP VPN-Client (Android)	CP / SSC
SOFTNET Security Client 2008	x	x	x
SOFTNET Security Client V3.0	x	x	x
SOFTNET Security Client V4.0	x	x	x
SCALANCE M / VPN-Gerät	-	x	x
NCP VPN-Client (Android)	-	x	x

6.3.2 Unterstützte Tunnelkommunikationsbeziehungen

Bedeutung

Die folgenden Tabellen geben an, welche Tunnel-Schnittstellen miteinander einen Tunnel aufbauen können. Dabei wird unterschieden, ob sich die SCALANCE S Baugruppe im Routing- oder im Bridge-Modus befindet.

Unabhängig davon, über welche Schnittstelle der VPN-Tunnel aufgebaut wird, können standardmäßig immer die Teilnehmer der internen Subnetze der Security-Baugruppen miteinander kommunizieren. Soll die Kommunikation über den VPN-Tunnel zusätzlich noch in andere Subnetze erfolgen, so können diese über das Register "VPN" in den erweiterten Baugruppeneigenschaften für die Tunnelkommunikation freigegeben werden, siehe folgendes Kapitel:

- Weitere Teilnehmer und Subnetze für den VPN-Tunnel konfigurieren (Seite 228)

Subnetze, die für die Tunnelkommunikation freigegeben werden müssen, sind:

- Subnetz an der externen Schnittstelle (wenn externe Schnittstelle nicht VPN-Endpunkt ist)
- Subnetz an DMZ-Schnittstelle (wenn DMZ-Schnittstelle nicht VPN-Endpunkt ist)
- Weitere durch Router erreichbare Subnetze an den verschiedenen Schnittstellen (wenn diese nicht VPN-Endpunkte sind)

Tabelle 6- 2 Tunnelkommunikation zwischen CPs, SCALANCE M Baugruppen, SOFTNET Security Clients und SCALANCE S Baugruppen im Routing-Modus

	Responder-Schnittstelle				
Initiator-Schnittstelle	**Extern (SCALANCE M875)**	**Extern (SCALANCE M-800)**	**GBit, IE (CP)**	**Extern (SCALANCE S)**	**DMZ (SCALANCE S623 / S627-2M)**
PC/PG (SSC)	x	x	x	x	x
Extern (SCALANCE M875)	-	x	x	x	x
Extern (SCALANCE M-800)	-	x	x	x	x
GBit, IE (CP)	-	-	x	x	x
Extern (SCALANCE S)	-	-	x	x	x
DMZ (SCALANCE S623 / S627-2M)	-	-	x	x	x

x wird unterstützt

- wird nicht unterstützt

Tabelle 6- 3 Tunnelkommunikation zwischen CPs, SOFTNET Security Clients und SCALANCE S Baugruppen im Bridge-Modus

	Responder-Schnittstelle		
Initiator-Schnittstelle	**GBit, IE (CP)**	**Extern (SCALANCE S)**	**DMZ (SCALANCE S623 / S627-2M)**
PC/PG (SSC)	x	x	-
GBit, IE (CP)	x	x	-
Extern (SCALANCE S)	x	x	-
DMZ (SCALANCE S623 / S627-2M)	-	-	-

x wird unterstützt

- wird nicht unterstützt

6.3.3 VPN-Gruppen anlegen und Baugruppen zuordnen

Voraussetzung

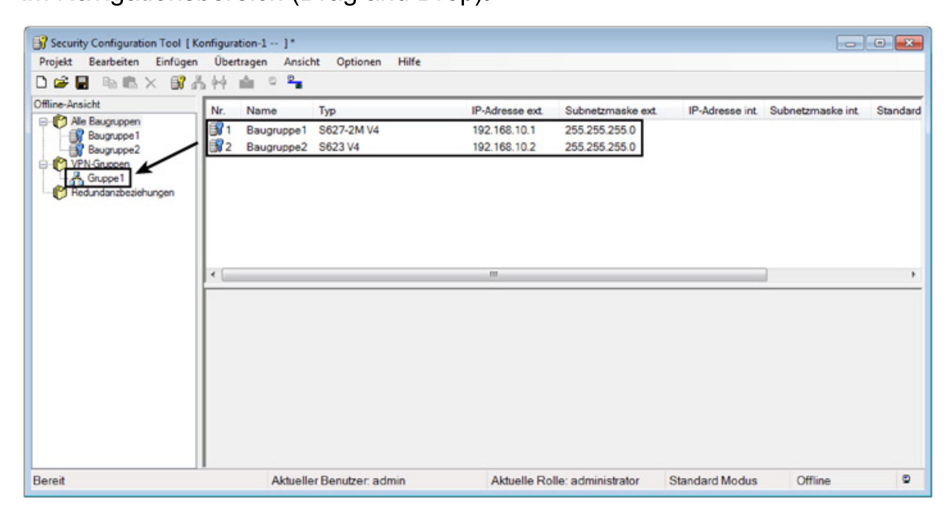
Hinweis

Aktuelles Datum und aktuelle Uhrzeit auf den Baugruppen

Achten Sie bei der Verwendung von gesicherter Kommunikation (z. B. HTTPS, VPN...) darauf, dass die betroffenen Baugruppen über die aktuelle Uhrzeit und das aktuelle Datum verfügen. Die verwendeten Zertifikate werden sonst als nicht gültig ausgewertet und die gesicherte Kommunikation funktioniert nicht.

So erreichen Sie diese Funktion

1. Legen Sie über den Menübefehl "Einfügen" > "Gruppe" eine VPN-Gruppe an.
2. Ordnen Sie der VPN-Gruppe die Baugruppen, SOFTNET Security Clients, VPN-Geräte und NCP VPN-Clients (Android) zu, die zu einer VPN-Gruppe gehören sollen. Ziehen Sie hierzu mit der Maus die Baugruppen im Inhaltsbereich auf die gewünschte VPN-Gruppe im Navigationsbereich (Drag and Drop).



Eigenschaften projektieren

Wie bei der Konfiguration von Baugruppen wirken sich auch bei der Konfiguration von VPN-Gruppen die beiden wählbaren Bedienungssichten im Security Configuration Tool aus:

- **Standard Modus**

  Im Standard Modus belassen Sie es bei den vom System vergebenen Voreinstellungen. Auch ohne Expertenwissen können Sie so IPsec-Tunnel konfigurieren und sichere Datenkommunikation betreiben.

- **Erweiterter Modus**

  Der Erweiterte Modus bietet Ihnen Einstellungsmöglichkeiten zur spezifischen Konfiguration der Tunnelkommunikation.

Alle projektierten VPN-Gruppen mit ihren Eigenschaften anzeigen

- Selektieren Sie im Navigationsbereich das Objekt "VPN-Gruppen".

Folgende Eigenschaften der Gruppen werden spaltenweise angezeigt:

Eigenschaft/Spalte	Bedeutung	Kommentar/Auswahl
Name	Gruppenname	Frei wählbar
Authentifizierung	Authentifizierungstyp	• Preshared Key • Zertifikat
Gruppenzugehörigkeit bis	Lebensdauer von Zertifikaten	Siehe Abschnitt "Lebensdauer von Zertifikaten einstellen"
Kommentar	Kommentar	Frei wählbar

Lebensdauer von Zertifikaten einstellen

Öffnen Sie den Dialog, in dem Sie das Ablaufdatum des Zertifikats eingeben können, wie folgt:

1. Selektieren Sie im Navigationsbereich die zugehörige VPN-Gruppe, für die Sie ein Zertifikat konfigurieren möchten.
2. Klicken Sie mit der rechten Maustaste auf die Baugruppe im Inhaltsbereich und wählen Sie im Kontextmenü den Befehl "Neues Zertifikat...".

Hinweis

Ablauf eines Zertifikats

Die Kommunikation durch den VPN-Tunnel läuft nach Ablauf des Zertifikats weiter, bis der Tunnel abgebaut wird oder die SA-Lebensdauer abläuft. Weitere Informationen zu Zertifikaten finden Sie in folgendem Kapitel:

- Zertifikate verwalten (Seite 83)

6.4 Tunnelkonfiguration im Standard Modus

Dialog zur Anzeige der Standardwerte öffnen

1. Markieren Sie die VPN-Gruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...".

Die Anzeige der VPN-Gruppeneigenschaften ist identisch zur Anzeige im Erweiterten Modus, jedoch können Sie die Werte im Standard Modus nicht verändern.

6.5 Tunnelkonfiguration im Erweiterten Modus

Der Erweiterte Modus bietet Ihnen Einstellmöglichkeiten zur spezifischen Konfiguration der Tunnelkommunikation.

In den Erweiterten Modus umschalten

Schalten Sie das Projekt für alle in diesem Kapitel beschriebenen Funktionen in den Erweiterten Modus ein.

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.

Abhilfe SCT Standalone: Sie schließen das Projekt ohne zu speichern und öffnen Sie es erneut.

6.5.1 VPN-Gruppeneigenschaften projektieren

VPN-Gruppeneigenschaften

Hinweis

IPsec-Kenntnisse erforderlich

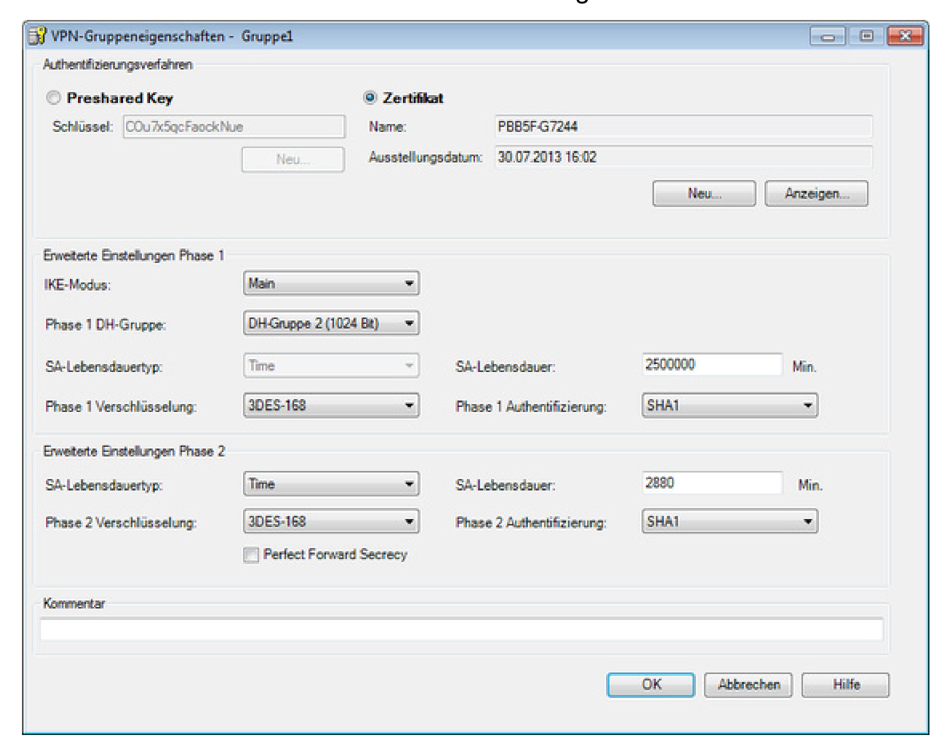
Um diese Parameter einstellen zu können, benötigen Sie IPsec-Kenntnisse. Wenn Sie keine Einstellungen vornehmen bzw. verändern, gelten die Standardeinstellungen des Standard Modus.

Im Erweiterten Modus sind folgende VPN-Gruppeneigenschaften projektierbar:

- Authentifizierungsverfahren
- IKE-Einstellungen (Dialogbereich: Erweiterte Einstellungen Phase 1)
- IPsec-Einstellungen (Dialogbereich: Erweiterte Einstellungen Phase 2)

So erreichen Sie diese Funktion

1. Markieren Sie im Navigationsbereich die zu bearbeitende VPN-Gruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften…".



3. Wählen Sie aus, ob für die Authentifizierung ein Preshared Key oder Zertifikat verwendet werden soll. Weitere Informationen hierzu finden Sie in folgendem Kapitel:
   – Authentifizierungsverfahren (Seite 203).

Parameter für erweiterte Einstellungen Phase 1

Phase 1: IKE-Aushandlung der Security Association (SA) für Phase 2:

Stellen Sie hier die Parameter für die Aushandlung der Sicherheitsparameter ein, die in Phase 2 verwendet werden:

Parameter	Beschreibung
IKE-Modus	• Main Mode • Aggressive Mode Der Unterschied zwischen Main- und Aggressive Mode ist die "Identity-Protection", die im Main-Mode verwendet wird. Die Identität wird im Main-Mode verschlüsselt übertragen, im Aggressive-Mode nicht.
Phase 1 DH-Gruppe	Wählbare Gruppen für den Diffie-Hellman-Schlüsselaustausch: • Group 1 • Group 2 • Group 5 • Group 14

Parameter	Beschreibung
SA-Lebensdauertyp	Phase 1 Security Association (SA): • Time: Zeitbegrenzung in Minuten Die Nutzdauer für das aktuelle Schlüsselmaterial wird zeitlich begrenzt. Nach Ablauf der Zeit wird das Schlüsselmaterial neu ausgehandelt.
SA-Lebensdauer	Numerischer Wert: Wertebereich für Time: 1440 ... 2500000 Minuten (Standard: 2500000)
Phase 1 Verschlüsselung	Verschlüsselungs-Algorithmus: • DES*: Data Encryption Standard (56 Bit Schlüssellänge, Modus CBC) • 3DES-168: Dreifach-DES (168 Bit Schlüssellänge, Modus CBC) • AES-128, 192, 256: Advanced Encryption Standard (128, 192 Bit oder 256 Bit Schlüssellänge, Modus CBC)
Phase 1 Authentifizierung	Authentisierungs-Algorithmus: • MD5: Message Digest Algorithm 5 • SHA1: Secure Hash Algorithm 1

* DES ist ein unsicherer Verschlüsselungsalgorithmus. Er sollte nur aus Gründen der Abwärtskompatibilität verwendet werden.

Parameter für erweiterte Einstellungen Phase 2

Phase 2: IKE-Aushandlung der Security Association (SA) für IPsec-Datenaustausch:

Stellen Sie hier die Parameter für die Aushandlung der Sicherheitsparameter ein, die für den IPsec-Datenaustausch mit ESP (Encapsulating Security Payload) und AH (Authentication Header) verwendet werden. Die Kommunikation in Phase 2 erfolgt bereits verschlüsselt.

Parameter	Beschreibung
SA-Lebensdauertyp	Phase 2 Security Association (SA): • Time: Zeitbegrenzung in Minuten Die Nutzdauer für das aktuelle Schlüsselmaterial wird zeitlich begrenzt. Nach Ablauf der Zeit wird das Schlüsselmaterial neu ausgehandelt. • Limit: Begrenzung des Datenvolumen in Mbyte
SA-Lebensdauer	Numerischer Wert: • Wertebereich für Time: 60 ... 16666666 Minuten (Standard: 2880) • Wertebereich für Limit: 2000 ... 500000 Mbyte (Standard: 4000)
Phase 2 Verschlüsselung	Verschlüsselungs-Algorithmus: • DES*: Data Encryption Standard (56 Bit Schlüssellänge, Modus CBC) • 3DES-168: Dreifach-DES (168 Bit Schlüssellänge, Modus CBC) • AES-128: Advanced Encryption Standard (128 Bit Schlüssellänge, Modus CBC)

Parameter	Beschreibung
Phase 2 Authentifizierung	Authentisierungs-Algorithmus: • MD5: Message Digest Algorithm 5 • SHA1: Secure Hash Algorithm 1
Perfect Forward Secrecy	Wenn Sie dieses Kontrollkästchen aktivieren, werden für die Neuberechnung der Schlüssel neue Diffie Hellmann Public Key Values ausgetauscht. Wenn das Kontrollkästchen deaktiviert ist, werden für die Neuberechnung der Schlüssel die bereits in Phase 1 ausgetauschten Werte verwendet.

* DES ist ein unsicherer Verschlüsselungsalgorithmus. Er sollte nur aus Gründen der Abwärtskompatibilität verwendet werden.

6.5.2 Baugruppe in konfigurierte VPN-Gruppe aufnehmen

Die projektierten Gruppeneigenschaften werden für Baugruppen, die in eine bestehende VPN-Gruppe aufgenommen werden, übernommen.

Aktive Teilnehmer in eine VPN-Gruppe aufnehmen

Wird ein aktiver Teilnehmer in eine bestehende VPN-Gruppe hinzugefügt, so kann dieser die Gruppenteilnehmer erreichen, ohne dass Sie das Projekt erneut auf alle Teilnehmer der VPN-Gruppe laden.

Hinweis

Wenn Sie einen aktiven Teilnehmer aus einer bestehenden VPN-Gruppe entfernen, kann dieser immer noch eine Verbindung zu den Gruppenteilnehmern aufbauen, auch wenn Sie das Projekt erneut auf alle Teilnehmer der VPN-Gruppe geladen haben.

Soll der entfernte aktive Teilnehmer keine Verbindung mehr aufbauen können, erneuern Sie das CA-Zertifikat der VPN-Gruppe und laden Sie das Projekt erneut auf die Teilnehmer der VPN-Gruppe.

Erneuert werden kann das CA-Zertifikat der VPN-Gruppe in den Gruppeneigenschaften der VPN-Gruppe oder im Zertifikatsmanager, Register "Zertifizierungsstellen".

So gehen Sie vor

Beim Vorgehen müssen Sie folgendermaßen unterscheiden:

- **Fall a:** Wenn Sie die Gruppeneigenschaften nicht geändert haben und die hinzuzufügende Baugruppe die Verbindung zu den bereits konfigurierten Baugruppen aktiv aufbaut:

1. Fügen Sie die neue Baugruppe der VPN-Gruppe hinzu.
2. Laden Sie die Konfiguration auf die neue Baugruppe.

- **Fall b:** Wenn Sie die Gruppeneigenschaften geändert haben oder die hinzuzufügende Baugruppe die Verbindung zu den bereits konfigurierten Security-Baugruppen nicht aktiv aufbaut:

1. Fügen Sie die neue Baugruppe der VPN-Gruppe hinzu.
2. Laden Sie die Konfiguration auf alle Baugruppen, die zur VPN-Gruppe gehören.

Vorteil in Fall a

Bereits vorhandene, in Betrieb genommene Baugruppen müssen nicht neu projektiert und geladen werden. Die laufende Kommunikation wird nicht beeinflusst oder unterbrochen.

Einstellungen für Teilnehmer mit unbekannter IP-Adresse

Teilnehmer, bei denen zum Projektierungszeitpunkt die IP-Adresse unbekannt ist (Unknown Peers), können in eine bestehende VPN-Gruppe eingefügt werden. Da sich die Teilnehmer meist im mobilen Einsatz befinden und die IP-Adresse dynamisch beziehen (z. B. ein SOFTNET Security Client oder SCALANCE M), kann der VPN-Tunnel nur aufgebaut werden, wenn Sie die Parametereinstellungen für Phase 1 entsprechend einer der folgenden Tabellen vornehmen. Verwenden Sie andere Einstellungen, können Sie keinen VPN-Tunnel zum Endgerät aufbauen.

Tabelle 6- 4 Verschlüsselungsparameter 1

Parameter	Einstellung
Phase 1 Verschlüsselung	AES-256
Phase 1 DH-Gruppe	Group2
Phase 1 Authentifizierung	SHA1
Authentifizierungsmethode	Zertifikat
SA-Lebensdauer	1440 … 2500000 Minuten

Tabelle 6- 5 Verschlüsselungsparameter 2

Parameter	Einstellung
Phase 1 Verschlüsselung	3DES-168
Phase 1 DH-Gruppe	Group2
Phase 1 Authentifizierung	SHA1
Authentifizierungsmethode	Zertifikat
SA-Lebensdauer	1440 … 2500000 Minuten

Tabelle 6- 6 Verschlüsselungsparameter 3

Parameter	Einstellung
Phase 1 Verschlüsselung	DES
Phase 1 DH-Gruppe	Group2
Phase 1 Authentifizierung	MD5
Authentifizierungsmethode	Zertifikat
SA-Lebensdauer	1440 … 2500000 Minuten

Tabelle 6- 7 Verschlüsselungsparameter 4

Parameter	Einstellung
Phase 1 Verschlüsselung	3DES-168
Phase 1 DH-Gruppe	Group2
Phase 1 Authentifizierung	SHA1
Authentifizierungsmethode	Preshared Key
SA-Lebensdauer	1440 … 2500000 Minuten

Zusätzliche Einschränkungen für den SOFTNET Security Client

Für den SOFTNET Security Client gelten zusätzlich die folgenden Einschränkungen:

Parameter	Einstellung / Besonderheit
Phase 1 Verschlüsselung	AES-256 nur bei Windows 7 möglich
Phase 1 SA-Lebensdauer	1440 ... 2879 Minuten
SA-Lebensdauertyp	Muss für beide Phasen identisch gewählt werden
Phase 2 Verschlüsselung	Kein AES-128 möglich
Phase 2 SA-Lebensdauer	60 ... 2879 Minuten
Phase 2 Authentifizierung	Kein MD5 möglich

6.5.3 Baugruppenspezifische VPN-Eigenschaften projektieren

Bedeutung

Für den Datenaustausch über die IPsec-Tunnel im VPN können Sie folgende baugruppenspezifische Eigenschaften konfigurieren:

- Dead-Peer-Detection SCA. M
- Erlaubnis zur Initiierung des Verbindungsaufbaus M875
- WAN-IP-Adresse / FQDN zur Kommunikation über Internet-Gateways M875
- VPN-Knoten SCA. M

Voraussetzungen

- Im Register "VPN" können Sie nur Einstellungen vornehmen, wenn sich die zu konfigurierende Baugruppe in einer VPN-Gruppe befindet.
- Der Dialogbereich "VPN-Knoten" im Register "VPN" wird nur angezeigt, wenn sich das Projekt im Erweiterten Modus befindet. SCA. M

So erreichen Sie diese Funktion

1. Markieren Sie die zu bearbeitende Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "VPN".

   Die hier vorgenommenen Einstellungen werden standardmäßig als baugruppenweite Einstellungen für die verbindungsgranularen Einstellungen übernommen. Verbindungsgranulare Einstellungen können baugruppenweite Einstellungen überschreiben und sind im Detail-Fenster projektierbar. Weitere Informationen zur Projektierung verbindungsgranularer Einstellungen finden Sie in folgendem Kapitel:
   Verbindungsgranulare VPN-Eigenschaften projektieren (Seite 219)

Dead-Peer-Detection (DPD)

Standardmäßig ist DPD aktiviert. Damit DPD zuverlässig funktioniert, muss es auf beiden beteiligten Security-Baugruppen aktiviert sein.

Bei aktivierter DPD tauschen die Security-Baugruppen in einstellbaren Zeitintervallen zusätzliche Nachrichten aus, sofern gerade kein Datenverkehr über den VPN-Tunnel läuft. Hierdurch kann erkannt werden, ob die IPsec-Verbindung noch gültig ist oder eventuell neu aufgebaut werden muss. Besteht keine Verbindung mehr, werden die "Security Associations" (SA) von Phase 2 vorzeitig beendet. Bei deaktivierter DPD wird die SA erst nach Ablauf der SA-Lebensdauer beendet. Zur Einstellung der SA-Lebensdauer, siehe folgendes Kapitel:
VPN-Gruppeneigenschaften projektieren (Seite 210)

Erlaubnis zur Initiierung des Verbindungsaufbaus

Sie können die Erlaubnis zur Initiierung des VPN-Verbindungsaufbaus auf bestimmte Baugruppen im VPN beschränken.

Maßgebend für die Einstellung des beschriebenen Parameters ist die Vergabe der Adresse für das Gateway der zu projektierenden Baugruppe. Bei einer statisch vergebenen IP-Adresse kann die Baugruppe von der Gegenstelle gefunden werden. Bei dynamisch vergebener, und daher sich ständig ändernder IP-Adresse, kann die Gegenstelle nicht ohne Weiteres eine Verbindung aufbauen.

Modus	Bedeutung
Starte Verbindung zur Gegenstelle (Initiator/Responder) (Standard)	Bei dieser Option ist die Baugruppe "aktiv", d. h. es wird versucht, zu einer Gegenstelle eine Verbindung herzustellen. Die Annahme von Anfragen zum VPN-Verbindungsaufbau ist ebenfalls möglich. Diese Option wird empfohlen, wenn die zu projektierende Baugruppe vom ISP eine dynamische IP-Adresse zugewiesen bekommt. Die Adressierung der Gegenstelle erfolgt über deren projektierte WAN-IP-Adresse, deren projektierte externe Baugruppen-IP-Adresse oder den projektierten FQDN.
Warte auf Gegenstelle (Responder)	Bei dieser Option ist die Baugruppe "passiv", d. h. es wird gewartet, bis der Verbindungsaufbau von der Gegenstelle initiiert wird. Diese Option wird empfohlen, wenn die zu projektierende Baugruppe vom ISP eine statische IP-Adresse zugewiesen bekommen hat.

Hinweis

Stellen Sie nicht alle Baugruppen einer VPN-Gruppe auf "Warte auf Gegenstelle", da sonst keine Verbindung aufgebaut wird.

WAN-IP-Adresse / FQDN - Adressen der Baugruppen und Gateways bei einem VPN über Internet

Beim Betrieb eines VPN mit IPsec-Tunnel über das Internet sind in der Regel zusätzliche IP-Adressen für die Internet-Gateways, z. B. DSL-Router, erforderlich. Den einzelnen Security- oder SCALANCE M-Baugruppen müssen die öffentlichen IP-Adressen der Partner-Baugruppen, welche über das Internet erreicht werden sollen, im VPN bekannt sein.

Hinweis

Wenn Sie einen DSL-Router als Internet-Gateway nutzen, müssen an diesem mindestens die folgenden Ports gemäß der Angaben in der zugehörigen Dokumentation freigeschaltet und die Datenpakete an die Baugruppe weitergeleitet werden:

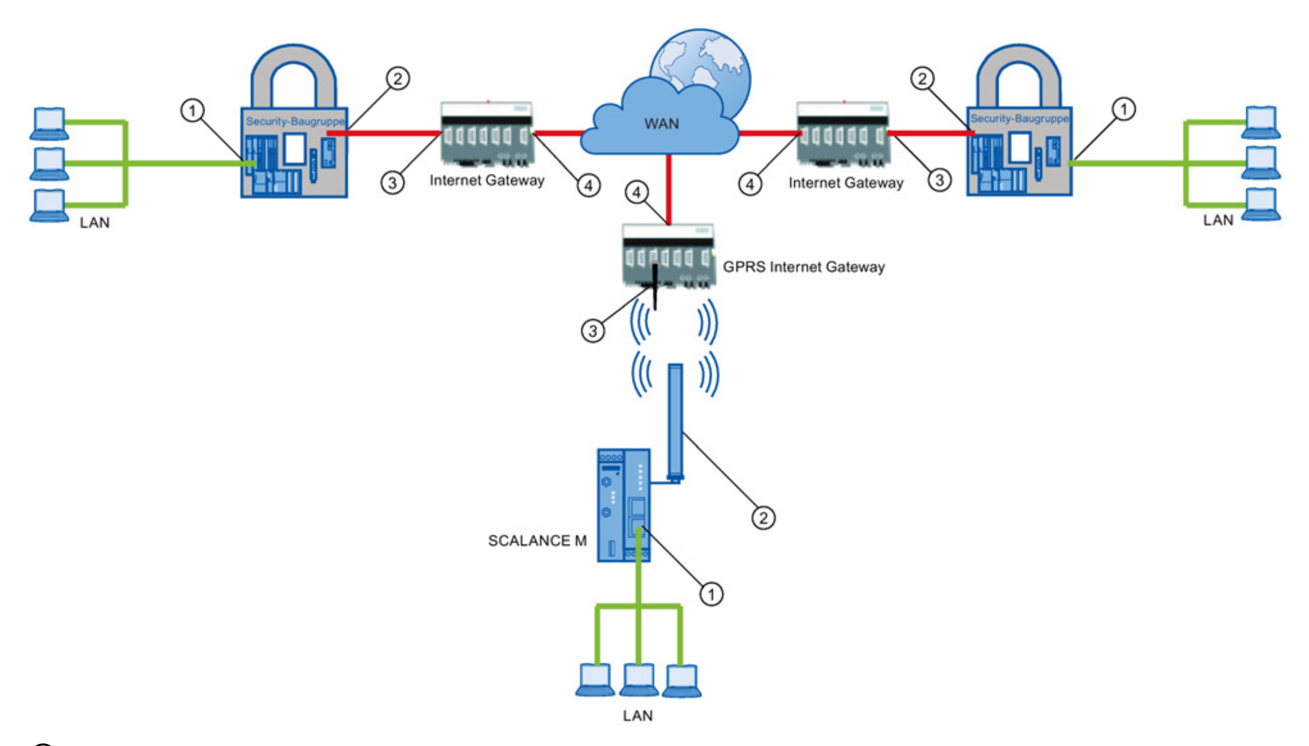
- Port 500 (ISAKMP)
- Port 4500 (NAT-T)

Hierzu besteht die Möglichkeit, in der Konfiguration von Security- oder SCALANCE M Baugruppen eine "WAN-IP-Adresse" festzulegen. Beim Laden der Baugruppenkonfiguration werden den Gruppenteilnehmern dann die WAN-IP-Adressen der Partner-Baugruppen mitgeteilt. Alternativ zu einer WAN-IP-Adresse können Sie auch einen FQDN eintragen.

Falls Sie gleichzeitig dynamisches DNS auf der Security-Baugruppe konfiguriert haben, muss dieser FQDN mit dem im Register "DNS" eingetragenen FQDN übereinstimmen, der bei einem Anbieter für dynamisches DNS registriert ist.

Ob die externe IP-Adresse, die IP-Adresse der DMZ-Schnittstelle (nur SCALANCE S623 / S627-2M) oder die WAN-IP-Adresse / der FQDN verwendet werden soll, können Sie in den verbindungsgranularen VPN-Eigenschaften festlegen. Weitere Informationen zu verbindungsgranularen VPN-Eigenschaften finden Sie in folgendem Kapitel: Verbindungsgranulare VPN-Eigenschaften projektieren (Seite 219)

Tragen Sie hier keinen Zugangspunkt ein, wird als VPN-Endpunkt die externe IP-Adresse oder die IP-Adresse der DMZ-Schnittstelle (nur SCALANCE S623/S627-2M) verwendet. Für SCALANCE M-800 Baugruppen, die als Responder projektiert sind, muss ein Zugangspunkt angegeben werden.



① IP-Adresse intern - einer Security-Baugruppe
② IP-Adresse extern - einer Baugruppe
③ IP-Adresse eines Internet Gateways (z. B. GPRS-Gateway)
④ IP-Adresse (WAN-IP-Adresse) eines Internet Gateways (z. B. DSL-Router)

VPN-Knoten konfigurieren

Im Dialogbereich "VPN-Knoten" geben Sie Subnetze oder Teilnehmer für die VPN-Tunnelkommunikation frei.

Welche Teilnehmer bzw. Subnetze freigegeben werden müssen und wie diese für die VPN-Tunnelkommunikation freigegeben werden, erfahren Sie in folgenden Kapiteln:

Weitere Teilnehmer und Subnetze für den VPN-Tunnel konfigurieren (Seite 228)

Interne Netzknoten konfigurieren (Seite 227)

6.5.4 Verbindungsgranulare VPN-Eigenschaften projektieren

Bedeutung

Während baugruppenspezifische VPN-Eigenschaften speziell für eine Baugruppe projektiert werden, beziehen sich verbindungsgranulare VPN-Eigenschaften speziell auf die VPN-Verbindungen einer Baugruppe. Wenn eine Baugruppe mehrere Tunnelverbindungen zu anderen Baugruppen aufbaut, kann mit Hilfe von verbindungsgranularen VPN-Eigenschaften beispielsweise konfiguriert werden, welche Verbindungen die Baugruppe initiiert und welche nicht.

Voraussetzungen

- Die Baugruppe ist Teilnehmer einer VPN-Gruppe.

So erreichen Sie diese Funktion

1. Selektieren Sie im Navigationsbereich die VPN-Gruppe, zu welcher die zu bearbeitende Baugruppe gehört.
2. Selektieren Sie im Inhaltsbereich die Baugruppe, deren Eigenschaften Sie projektieren wollen.

   Im Detail-Fenster können Sie nun die verbindungsgranularen VPN-Eigenschaften projektieren. Die voreingestellten Werte sind den baugruppenspezifischen VPN-Eigenschaften entnommen.

Parameter

Parameter	Bedeutung
Initiator/Responder	Festlegung der Erlaubnis zur Initiierung des Verbindungs-aufbaus.
Partner-Baugruppe	Anzeige des Baugruppennamens der Partner-Baugruppe.
Art der übertragenen Pakete	Anzeige des Layers, auf dem die Pakete übertragen wer-den.
Lokale Schnittstelle	Festlegung der Schnittstelle, die als VPN-Endpunkt an der ausgewählten Baugruppe verwendet werden soll. Ist für die Baugruppe ein WAN-Zugangspunkt (IP-Adresse / FQDN) projektiert, kann dieser hier ebenfalls ausgewählt werden.
Partner-Schnittstelle	Festlegung der Schnittstelle, die als VPN-Endpunkt an der Partner-Baugruppe verwendet werden soll. Ist für die VPN-Gegenstelle ein WAN-Zugangspunkt (IP-Adresse / FQDN) projektiert, kann dieser hier ebenfalls ausgewählt werden.

6.6 Konfigurationsdaten für SCALANCE M Baugruppen



Bedeutung

Sie können die VPN-Informationen zur Parametrierung von SCALANCE M Baugruppen mit dem Security Configuration Tool generieren. Mit den generierten Dateien können Sie dann die SCALANCE M Baugruppen konfigurieren.

Folgende Dateitypen werden erzeugt:

- Exportdatei mit den Konfigurationsdaten
  - Dateityp: *.txt-Datei im ASCII-Format
  - Enthält die exportierten Konfigurationsinformationen für den SCALANCE M einschließlich einer Information über die zusätzlich erzeugten Zertifikate.
  - Exportdatei für SCALANCE M875 Baugruppen:

```
Konfiguration-1.Baugruppe1.txt - Editor
Datei  Bearbeiten  Format  Ansicht  ?

SCALANCE M875/MD741-1
{
Informationen für die Konfiguration des SCALANCE M875/MD741-1: Baugruppe1


--------------------------------------------------------------------------------
Verbindung zwischen Baugruppe1 und Baugruppe2

IPSec VPN > Zertifikate
    Gegenstellen Zertifikat hochladen: Konfiguration-1.Gruppe1.Baugruppe2.cer
    PKCS12 Datei (.p12) hochladen: Konfiguration-1.U701515CF@GE1C4.Baugruppe1.p12

IPSec VPN > Verbindungen > VPN Standard Modus - Einstellungen bearbeiten
    Adresse des VPN Gateways der Gegenstelle: 192.168.10.2
    Authentisierungsverfahren: X.509 Gegenstellenzertifikat
    Gegenstellen Zertifikat: Konfiguration-1.Gruppe1.Baugruppe2.cer
    Remote-ID: UA65D89FF@GE1C4
    Lokale ID: U701515CF@GE1C4

    Adresse des gegenüberliegenden Netzes: 192.168.8.0
    Netzmaske des gegenüberliegenden Netzes: 255.255.255.0
    Adresse des lokalen Netzes: 192.168.9.0
    Netzmaske des lokalen Netzes: 255.255.255.0

IPSec VPN > Verbindungen > IKE Bearbeiten

    Phase 1 - ISAKMP SA
    ISAKMP-SA Verschlüsselung: 3DES-168
    ISAKMP-SA Hash: SHA-1
    ISAKMP-SA Modus: Main Mode
    ISAKMP-SA Lebensdauer: 86400

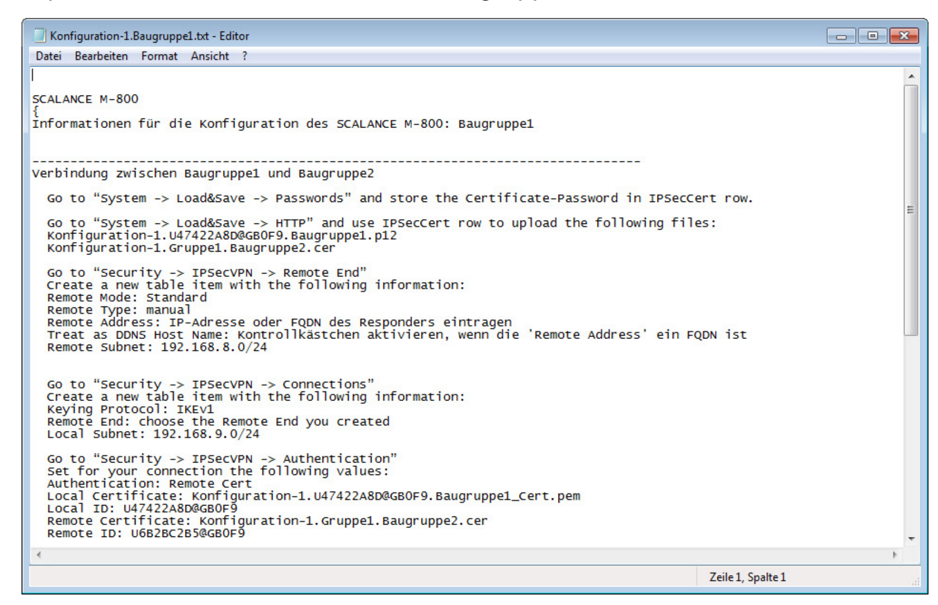
    Phase 2 - IPSec SA
    IPSec-SA Verschlüsselung: 3DES-168
    IPSec-SA Hash: SHA-1
    IPSec-SA Lebensdauer: 86400
    Perfect Forward Secrecy (PFS): Nein

    DH/PFS-Gruppe: DH-2 1024
    NAT-T: An

Zeile 38, Spalte 32
```



– Exportdatei für SCALANCE M-800 Baugruppen:



Konfiguration-1.Baugruppe1.txt - Editor

Datei Bearbeiten Format Ansicht ?

```
SCALANCE M-800
{
Informationen für die Konfiguration des SCALANCE M-800: Baugruppe1


--------------------------------------------------------------------------------
Verbindung zwischen Baugruppe1 und Baugruppe2

  Go to “System -> Load&Save -> Passwords” and store the Certificate-Password in IPSecCert row.

  Go to “System -> Load&Save -> HTTP” and use IPSecCert row to upload the following files:
  Konfiguration-1.U47422A8D@GB0F9.Baugruppe1.p12
  Konfiguration-1.Gruppe1.Baugruppe2.cer

  Go to “Security -> IPSecVPN -> Remote End”
  Create a new table item with the following information:
  Remote Mode: Standard
  Remote Type: manual
  Remote Address: IP-Adresse oder FQDN des Responders eintragen
  Treat as DDNS Host Name: Kontrollkästchen aktivieren, wenn die 'Remote Address' ein FQDN ist
  Remote Subnet: 192.168.8.0/24


  Go to “Security -> IPSecVPN -> Connections”
  Create a new table item with the following information:
  Keying Protocol: IKEv1
  Remote End: choose the Remote End you created
  Local Subnet: 192.168.9.0/24

  Go to “Security -> IPSecVPN -> Authentication”
  Set for your connection the following values:
  Authentication: Remote Cert
  Local Certificate: Konfiguration-1.U47422A8D@GB0F9.Baugruppe1_Cert.pem
  Local ID: U47422A8D@GB0F9
  Remote Certificate: Konfiguration-1.Gruppe1.Baugruppe2.cer
  Remote ID: U6B2BC2B5@GB0F9
```

Zeile 1, Spalte 1

- VPN-Gruppen-Zertifikate der Baugruppe
  - Dateityp des privaten Schlüssels: *.p12-Datei
  - Die Datei enthält das VPN-Gruppen-Zertifikat der Baugruppe und das zugehörige Schlüsselmaterial.
  - Der Zugriff ist passwortgeschützt.
- CA-Zertifikate von VPN-Gruppen
  - Dateityp: *.cer-Datei

Hinweis

Konfigurationsdateien werden nicht an die Baugruppe übertragen. Es wird eine ASCII-Datei generiert, mit der Sie die VPN-relevanten Eigenschaften des SCALANCE M konfigurieren können. Dazu muss sich die Baugruppe in mindestens einer VPN-Gruppe mit einer Security-Baugruppe oder einem SOFTNET Security Client ab V3.0 befinden.

Hinweis

Exportierte Konfigurationsdateien vor unberechtigtem Zugriff schützen

Aus dem Security Configuration Tool exportierte Konfigurationsdateien für SCALANCE M können sicherheitsrelevante Informationen enthalten. Stellen Sie deshalb sicher, dass diese Dateien vor unberechtigtem Zugriff geschützt sind. Dies ist insbesondere bei der Weitergabe der Dateien zu beachten.

Konfigurationsdateien generieren

1. Selektieren Sie die zu bearbeitende Baugruppe.
2. Wählen Sie den Menübefehl "Übertragen" > "An Baugruppe(n)...".
3. Geben Sie im folgenden Speicherdialog den Pfad- und Dateinamen der Konfigurationsdatei an und klicken Sie auf die Schaltfläche "Speichern".
4. Geben Sie im folgenden Dialog an, ob für das VPN-Gruppen-Zertifikat der Baugruppe ein eigenes Passwort erstellt werden soll.

   Wenn Sie "Nein" wählen, wird als Passwort der Projektname vergeben (z. B. SCALANCE_M_Konfiguration1), nicht das Projektpasswort.

   Wenn Sie "Ja" wählen (empfohlen), müssen Sie im darauf folgenden Dialog ein Passwort vergeben.

Ergebnis: Die Dateien (und Zertifikate) werden in dem von Ihnen angegebenen Verzeichnis abgespeichert.

Hinweis

Weitere Informationen zur Konfiguration finden Sie in den Betriebsanleitungen der entsprechenden SCALANCE M Baugruppen.

6.7 Konfigurationsdaten für VPN-Geräte

Bedeutung

Sie können die VPN-Informationen zur Parametrierung eines VPN-Geräts mit dem Security Configuration Tool generieren. Mit den generierten Dateien können Sie dann das VPN-Gerät konfigurieren.

Folgende Dateien werden erzeugt:

- Exportdatei mit den Konfigurationsdaten
  - Dateityp: *.txt-Datei im ASCII-Format
  - Enthält die exportierten Konfigurationsinformationen für das VPN-Gerät einschließlich einer Information über die zusätzlich erzeugten Zertifikate.

```
VPN-Geraet_deu - Editor
Datei  Bearbeiten  Format  Ansicht  ?
Informationen für die Konfiguration eines anderen VPN-fähigen Produktes: Modul2


--------------------------------------------------------------------------------
Verbindung zwischen Modul2 und Modul1

Phase 1:
> IP-Adresse des VPN-Partners: 192.168.10.1
> Dieses Modul ist konfiguriert als: Initiator und Responder, das VPN-Gerät muss sowohl die Verbindung initiieren als auch auf die Verbindung warten
> Authentisierungsverfahren: Certificate
> Negotiation Method: Main Mode
> Identifikation:
    Local ID: U6BE829C9@GA9B3
    Remote ID: U15D2DDF1@GA9B3
    Identifikationstyp: User-FQDN
> Verschlusselung: 3DES-168
> Hash: SHA-1
> DH-Group: Group2
> Lebensdauer: 150000000
> NAT-T: on / off
> Zertifikat des VPN-Partners: Konfiguration-1.Gruppe1.Modul1.crt
> Zertifikate des Moduls:
    > PEM-Format: Konfiguration-1.U6BE829C9@GA9B3.Modul2.pem
    > PKCS12-Format (mit privatem Schlüssel): Konfiguration-1.U6BE829C9@GA9B3.Modul2.p12

Phase 2:
> Freigegebene lokale Netzadresse: 192.168.9.0
> Freigegebenes lokales Subnetz: 255.255.255.0
> Über IPSec freizugebende Subnetze:
> Freigegebene Netzadresse der Gegenstelle : 192.168.3.0
> Freigegebenes Subnetz der Gegenstelle: 255.255.255.0
> Protokol: ESP
> Verschlüsselung: 3DES-168
> Hash: SHA-1
> Perfect Forward Secrecy (PFS): Nein
> SA Lebensdauer-Typ: Time
> SA Lebensdauer: 172800
```

Bild 6-1 Exportdatei für ein VPN-Gerät

- VPN-Gruppen-Zertifikate des VPN-Geräts
- VPN-Gruppen-Zertifikate von Partnerbaugruppen
- Private Schlüssel
- CA-Zertifikate von VPN-Gruppen

Dateitypen konfigurieren

Für VPN-Geräte können Sie die Dateitypen bestimmen, unter welchen die generierten Daten abgespeichert werden.

Selektieren Sie hierzu das zu bearbeitende VPN-Gerät und wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...".

- VPN-Gruppen-Zertifikate des VPN-Geräts
  - *.crt-Datei: Base64-kodiertes Zertifikat
  - *.pem-Datei: Base64-kodiertes Zertifikat
  - *.pem-Datei: Binärkodiertes Zertifikat
- VPN-Gruppen-Zertifikate von Partnerbaugruppen:
  - *.crt-Datei: Base64-kodiertes Zertifikat
  - *.pem: Base64-kodiertes Zertifikat
  - *.pem: Binärkodiertes Zertifikat
- Private Schlüssel:
  - *.p12-Datei: Passwortgeschütztes PKCS12 Archiv mit privatem Schlüssel
  - *.key: Ungeschützter Base64-kodierter privater Schlüssel
- CA-Zertifikate von VPN-Gruppen:
  - *.crt-Datei: Base64-kodiertes Zertifikat
  - *.pem-Datei: Base64-kodiertes Zertifikat
  - *.pem-Datei: Binärkodiertes Zertifikat

Hinweis

Konfigurationsdateien werden nicht an das VPN-Gerät übertragen. Es wird eine ASCII-Datei generiert, mit der Sie das VPN-Gerät konfigurieren können. Dazu muss sich das VPN-Gerät in mindestens einer VPN-Gruppe mit einer Security-Baugruppe oder einem SOFTNET Security Client ab V3.0 befinden.

Konfigurationsdateien generieren

1. Markieren Sie das zu bearbeitende VPN-Gerät.
2. Wählen Sie den Menübefehl "Übertragen" > "An Baugruppe(n)...".
3. Geben Sie im folgenden Speicherdialog den Pfad- und Dateinamen der Konfigurationsdatei an und klicken Sie auf die Schaltfläche "Speichern".
4. Geben Sie im folgenden Dialog an, ob für die beiden erstellten Zertifikatdateien ein eigenes Passwort erstellt werden soll.

   Wenn Sie "Nein" wählen, wird als Passwort der Projektname vergeben (z. B. VPN-Projekt_02), nicht das Projektpasswort.

   Wenn Sie "Ja" wählen (empfohlen), müssen Sie im darauf folgenden Dialog ein Passwort vergeben.

Ergebnis: Die Dateien (und Zertifikate) werden in dem von Ihnen angegebenen Verzeichnis abgespeichert.

6.8 Konfigurationsdaten für NCP VPN-Clients (Android)

NCP Secure VPN Client for Android

Der NCP Secure Android Client ermöglicht eine hochsichere VPN-Verbindung zu zentralen Datennetzen von Firmen und Organisationen. Der Zugriff ist auf mehrere unterschiedliche Datennetze mit jeweils eigenem VPN-Profil möglich.

Auf Basis des IPsec-Standards können Tablets und Smartphones verschlüsselte Datenverbindungen zu VPN Gateways aller namhaften Anbieter herstellen.

Der Client ist in zwei Varianten über den Google Play Store beziehbar:

- NCP Secure VPN Client for Android (Authentifizierung mit Preshared Key)
- NCP Secure VPN Client Premium for Android (Authentifizierung mit Preshared Key oder Zertifikat)

Weitere Informationen zu den NCP Secure Android Clients finden Sie hier:

NCP Secure VPN Client for Android (http://www.ncp-e.com/de/produkte/ipsec-vpn-client-fuer-android.html)

Bedeutung

Sie können die VPN-Informationen zur Parametrierung eines NCP VPN-Clients (Android) mit dem Security Configuration Tool generieren. Mit den generierten Dateien können Sie dann die NCP VPN-Client-Software konfigurieren.

Folgende Dateitypen werden erzeugt:

- Exportdatei mit den Konfigurationsdaten
  - Dateityp: *.ini-Datei im UTF-8-Format
  - Enthält die exportierten Konfigurationsinformationen für den NCP VPN-Client (Android) einschließlich einer Information über die zusätzlich erzeugten Zertifikate.
- VPN-Gruppen-Zertifikate der Baugruppe
  - Dateityp des privaten Schlüssels: *.p12-Datei
  - Die Datei enthält das VPN-Gruppen-Zertifikat der Baugruppe und das Schlüsselmaterial.
  - Der Zugriff ist passwortgeschützt.
- CA-Zertifikate von VPN-Gruppen:
  - Dateityp: *.crt-Datei

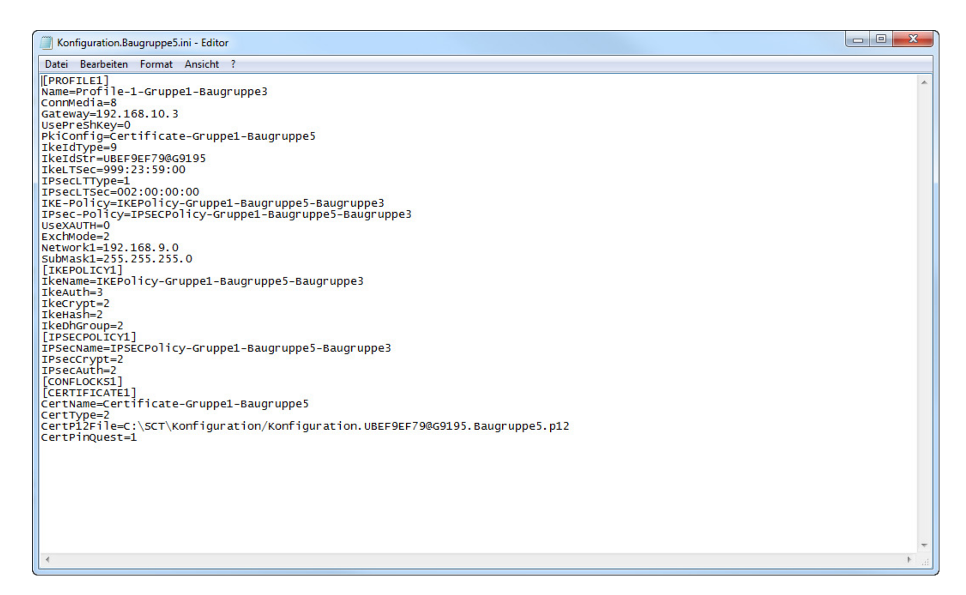


Bild 6-2 Export-Datei für einen NCP VPN-Client (Android)

Hinweis

Konfigurationsdateien werden nicht an den NCP VPN-Client (Android) übertragen. Es wird eine ASCII-Datei generiert, mit der Sie den NCP VPN-Client (Android) konfigurieren können. Dazu muss sich der NCP VPN-Client (Android) in mindestens einer VPN-Gruppe mit einer Security-Baugruppe befinden.

Konfigurationsdateien generieren

1. Markieren Sie im Inhaltbereich den zu bearbeitenden NCP VPN-Client (Android).
2. Wählen Sie den Menübefehl "Übertragen" > "An Baugruppe(n)...".
3. Geben Sie im folgenden Speicherdialog den Pfad- und Dateinamen der Konfigurationsdatei an und klicken Sie auf die Schaltfläche "Speichern".
4. Geben Sie im folgenden Dialog an, ob für die beiden erstellten Zertifikatdateien ein eigenes Passwort erstellt werden soll.

   Wenn Sie "Nein" wählen, wird als Passwort der Projektname vergeben (z. B. NCP-Projekt_02), nicht das Projektpasswort.

   Wenn Sie "Ja" wählen (empfohlen), müssen Sie im darauf folgenden Dialog ein Passwort vergeben.

Ergebnis: Die Dateien werden in dem von Ihnen angegebenen Verzeichnis abgespeichert.

6.9 Interne Netzknoten konfigurieren



Interne Netzknoten konfigurieren

Jeder Security-Baugruppe müssen die Netzknoten im gesamten internen Netz bekannt sein, um die Authentizität eines Telegramms feststellen zu können.

Die Security-Baugruppe muss sowohl seine eigenen internen Knoten kennen als auch die internen Knoten der Security-Baugruppen, mit denen sie zusammen in einer VPN-Gruppe ist. Diese Information wird auf einer Security-Baugruppe dazu verwendet, um zu bestimmen, welches Datenpaket in welchem Tunnel übertragen werden soll.

SCALANCE S

Eine SCALANCE S Baugruppe im Bridge-Modus bietet neben der statischen Konfiguration der Netzknoten auch die Möglichkeit, diese automatisch zu erlernen.
Wie Sie die Netzknoten statisch konfigurieren, erfahren Sie in folgendem Kapitel:
Weitere Teilnehmer und Subnetze für den VPN-Tunnel konfigurieren (Seite 228)

Informationen zum automatischen Lernen interner Netzknoten finden Sie in folgendem Kapitel:
Arbeitsweise des Lernmodus (Seite 229)

CP x43-1 Adv. und CP 1628

- CP x43-1 Adv.

  Wählen Sie aus, ob die Tunnelkommunikation zum CP und/oder zum internen Subnetz für VPN-Verbindungspartner im Routing-Modus (SCALANCE S / M / VPN-Gerät / NCP VPN-Client (Android)) erlaubt ist.

- CP 1628

  Tragen Sie die NDIS-Knoten ein, die durch den Tunnel von VPN-Verbindungspartnern im Routing-Modus (SCALANCE S / M / VPN-Gerät / NCP VPN-Client (Android)) erreichbar sein sollen.

6.9.1 Weitere Teilnehmer und Subnetze für den VPN-Tunnel konfigurieren



Bedeutung

Durch das Hinzufügen einer Security-Baugruppe zu einer VPN-Gruppe werden die lokalen, internen Netzknoten/Subnetze der Security-Baugruppe automatisch für die VPN-Tunnelkommunikation freigegeben. Um die Kommunikation über den VPN-Tunnel mit weiteren Subnetzen oder Teilnehmern eines weiteren Subnetzes zu ermöglichen, müssen diese Subnetze oder Teilnehmer für die VPN-Tunnelkommunikation über die Konfiguration freigegeben werden.

Ein Subnetz, das über die Konfiguration freigegeben werden kann, kann sein:

- Ein Subnetz, das über das lokale Netz an der internen Schnittstelle erreichbar ist, wenn ein VPN-Tunnel an der externen Schnittstelle oder an der DMZ-Schnittstelle terminiert.
- Ein Subnetz, das über die DMZ-Schnittstelle erreichbar ist, wenn ein VPN-Tunnel an der externen Schnittstelle terminiert.
- Ein Subnetz, das über die externe Schnittstelle erreichbar ist, wenn ein VPN-Tunnel an der DMZ-Schnittstelle terminiert.

Voraussetzung

Bevor die Teilnehmer oder Subnetze für die Tunnelkommunikation freigegeben werden können, müssen folgende Voraussetzungen erfüllt sein:

- Die Security-Baugruppe befindet sich in einer VPN-Gruppe.
- Der Dialogbereich "VPN-Knoten" im Register "VPN" wird nur angezeigt, wenn sich das Projekt im Erweiterten Modus befindet.

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.

Abhilfe SCT Standalone: Sie schließen das Projekt ohne zu speichern und öffnen Sie es erneut.

So erreichen Sie diese Funktion - Bridge-Modus

Anmerkung: Wenn Teilnehmer oder Subnetze an der DMZ-Schnittstelle (nur SCALANCE S623/S627-2M) freigegeben werden sollen, folgen Sie der Beschreibung für den Routing-Modus.

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "VPN".
   Die Freigabe von Teilnehmern und Subnetzen konfigurieren Sie im Dialogbereich "VPN-Knoten".
3. Wenn Sie komplette Subnetze für die Tunnelkommunikation freigeben wollen, tragen Sie diese im Register "Interne Subnetze" ein. Wenn Sie einzelne Teilnehmer für die Tunnelkommunikation freigeben wollen, tragen Sie die Teilnehmer im Register "Interne IP-Knoten" bzw. "Interne MAC-Knoten" ein.

Anmerkung: Damit hier angegebene Subnetze erreicht werden können, muss für diese auch ein Router im Register "Routing" eingetragen sein. Zudem muss die Firewall die Kommunikation mit den Teilnehmern erlauben.

So erreichen Sie diese Funktion - Routing-Modus

1. Markieren Sie die zu bearbeitende Security-Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "VPN".
   Die Freigabe von Subnetzen konfigurieren Sie im Dialogbereich "VPN-Knoten".
3. Tragen Sie im Register "Durch Tunnel erreichbare Subnetze" die Netz-ID und die Subnetzmaske des Subnetzes ein, das in die Tunnelkommunikation mit einbezogen werden soll.

Anmerkung: Damit hier angegebene Subnetze erreicht werden können, muss für diese auch ein Router im Register "Routing" eingetragen sein. Zudem muss die Firewall die Kommunikation mit den Subnetzen erlauben.

6.9.2 Arbeitsweise des Lernmodus



Teilnehmer für die Tunnelkommunikation automatisch finden (nur bei SCALANCE S im Bridge-Modus)

Ein großer Vorteil für die Konfiguration und den Betrieb der Tunnelkommunikation ist, dass SCALANCE S Baugruppen die Teilnehmer in internen Netzen selbsttätig auffinden können. Auf diese Weise müssen Sie die internen Netzknoten, die an der Tunnelkommunikation teilnehmen sollen, nicht manuell konfigurieren.

Neue Teilnehmer werden von der SCALANCE S Baugruppe im laufenden Betrieb erkannt. Die erkannten Teilnehmer werden an die SCALANCE S Baugruppe gemeldet, die zur selben VPN-Gruppe gehören. Dadurch ist der Datenaustausch innerhalb der Tunnel einer VPN-Gruppe jederzeit in beide Richtungen gewährleistet.

Voraussetzungen

Erkannt werden folgende Teilnehmer:

- IP-fähige Netzknoten

  IP-fähige Netzknoten werden gefunden, wenn eine ICMP-Antwort auf den ICMP-Subnetz-Broadcast gesendet wird.

  IP-Knoten hinter Routern sind auffindbar, wenn die Router ICMP-Broadcasts weiterleiten.

- ISO-Netzknoten

  Netzknoten, die zwar nicht IP-fähig sind, jedoch über ISO-Protokolle ansprechbar sind, können ebenfalls gelernt werden.

  Voraussetzung ist, dass sie auf XID- bzw. TEST-Telegramme antworten. TEST und XID (Exchange Identification) sind Hilfsprotokolle zum Informationsaustausch auf der Layer 2-Ebene. Durch das Versenden dieser Telegramme mit einer Broadcast-Adresse können diese Netzknoten ausfindig gemacht werden.

- PROFINET-Knoten

  Mit Hilfe von DCP (Discovery and basic Configuration Protocol) werden PROFINET-Knoten gefunden.

Netzknoten, die diese Bedingungen nicht erfüllen, müssen Sie statisch konfigurieren.

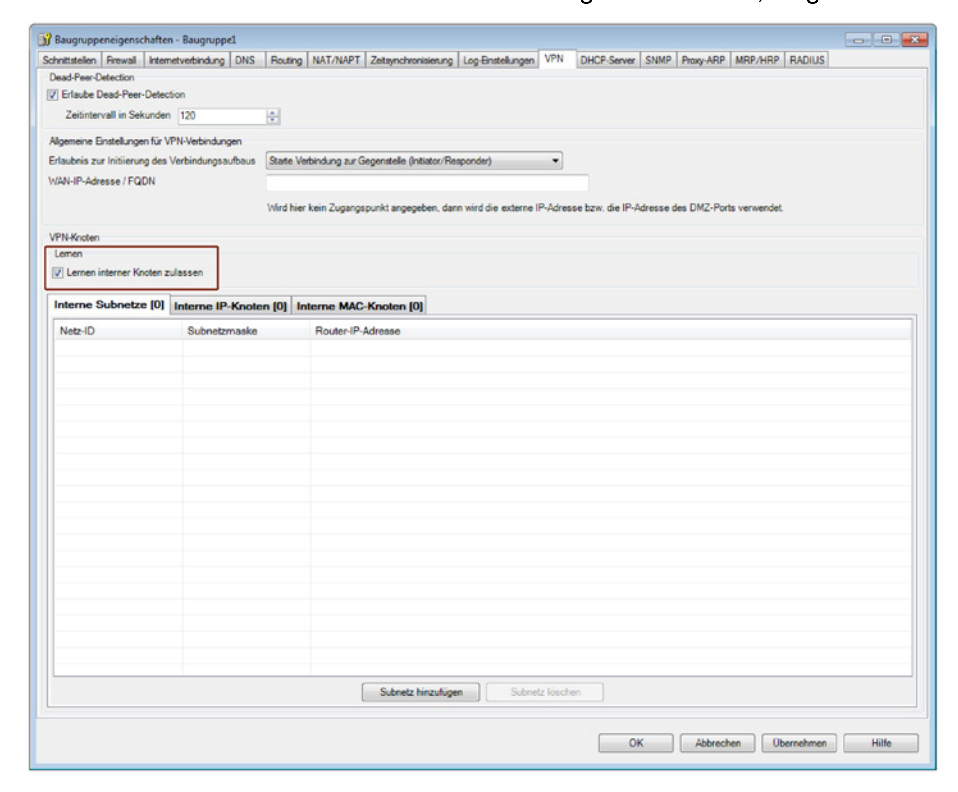
Hinweis

Kein Lernmodus bei VPN-Tunnel auf DMZ-Schnittstelle S62x

Das Lernen von internen Knoten wird nur auf Schnittstellen unterstützt, die im Bridge-Modus angebunden werden. Die DMZ-Schnittstelle wird stets im Routing-Modus angebunden.

So erreichen Sie die Funktion

1. Markieren Sie die zu bearbeitende SCALANCE S Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "VPN".



Wann ist es sinnvoll, den automatischen Lernmodus auszuschalten?

Die Standardeinstellungen für die Security-Baugruppe gehen davon aus, dass interne Netze stets sicher sind; das heißt auch, dass im Normalfall keine Netzknoten in das interne Netz zugeschaltet werden, die nicht vertrauenswürdig sind.

Das Ausschalten des Lernmodus ist sinnvoll, wenn das interne Netz statisch ist, d. h., wenn sich die Anzahl der internen Knoten und deren Adressen nicht ändern.

Mit Ausschalten des Lernmodus entfällt im internen Netz die Belastung des Mediums und der Netzknoten durch die Lerntelegramme. Auch die SCALANCE S Baugruppe wird leistungsfähiger, da sie nicht durch die Bearbeitung der Lerntelegramme belastet wird.

Anmerkung: Im Lernmodus werden alle Netzknoten im internen Netz erfasst. Die Angaben zum VPN-Mengengerüst beziehen sich nur auf die Netzknoten, die im internen Netz über VPN kommunizieren.

Hinweis

Werden im internen Netz mehr als 128 interne Knoten betrieben, wird damit das zulässige Mengengerüst überschritten und ein nicht erlaubter Betriebszustand erzeugt. Aufgrund der Dynamik im Netzwerkverkehr kommt es dann dazu, dass interne Knoten, die bereits gelernt wurden, wieder durch neue, bis jetzt noch nicht bekannte interne Knoten ersetzt werden.

Nicht lernbare Netzknoten

Es gibt Teilnehmer im internen Netz, die nicht gelernt werden können. Hierbei handelt es sich um Teilnehmer von Subnetzen, die sich am lokalen internen Netz der SCALANCE S Baugruppe (z.B. hinter Routern) befinden. Diese Subnetze können ebenfalls nicht gelernt werden. Nicht lernbare Teilnehmer und Subnetze müssen Sie im Erweiterten Modus statisch konfigurieren.

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.
Abhilfe SCT Standalone: Sie schließen das Projekt ohne zu speichern und öffnen Sie es erneut.

6.9.3 Anzeige der gefundenen internen Netzknoten

Alle gefundenen Netzknoten werden im Security Configuration Tool angezeigt.

1. Wechseln Sie in die Betriebsart "Online".
2. Wählen Sie den Menübefehl "Bearbeiten" > "Online Diagnose...", Register "Interne Knoten".

   Ergebnis: Die gefundenen internen Netzknoten werden angezeigt.

Router- und Firewallredundanz 7

7.1 Übersicht

Bedeutung

Durch Router- und Firewall-Redundanz können Ausfälle der Security-Baugruppen SCALANCE S623 ab V4 und SCALANCE S627-2M ab V4 während des Betriebs automatisiert kompensiert werden. Hierzu fassen Sie zwei Security-Baugruppen des Typs SCALANCE S623 oder SCALANCE S627-2M in einer Redundanzbeziehung zusammen und bestimmen dann, welches die im Normalbetrieb aktive Security-Baugruppe der Redundanzbeziehung sein soll. Fällt die aktive Security-Baugruppe aus, übernimmt die passive Security-Baugruppe automatisch deren Funktion als Firewall und (NAT-/NAPT-) Router. Um eine identische Konfiguration beider Security-Baugruppen zu gewährleisten, werden diese über deren DMZ-Schnittstellen miteinander verbunden und während des Betriebs in ihrer Konfiguration synchronisiert. Die DMZ-Schnittstellen der beteiligten Security-Baugruppen sind in diesem Fall nicht für andere Zwecke nutzbar.

Adressredundanz

Zusätzlich zu ihren jeweiligen Baugruppen-IP-Adressen teilen sich die beiden Security-Baugruppen an der externen und an der internen Schnittstelle jeweils eine gemeinsame IP-Adresse, damit bei Ausfall einer Security-Baugruppe keine Änderungen an den IP-Adressen notwendig sind. Deshalb müssen Sie für die externe und für die interne Schnittstelle der Redundanzbeziehung eine IP-Adresse projektieren.

Projektierung von Redundanzbeziehungen und eingebundenen Security-Baugruppen

Nachdem die Security-Baugruppen in eine Redundanzbeziehung eingebunden wurden, wird ein Teil der Baugruppeneigenschaften ausschließlich über die Redundanzbeziehung projektiert. Dieser Anteil der Baugruppeneigenschaften wird für die einzelnen Security-Baugruppen deaktiviert und ist erst wieder nach dem Entfernen der Security-Baugruppen aus der Redundanzbeziehung aktiv und editierbar. Folgende Eigenschaften werden über die Redundanzbeziehung projektiert:

- Grundeinstellungen der Redundanzbeziehung (Netzparameter, Primärbaugruppe)
- Firewall
- Routing
- NAT-/NAPT-Routing (kein 1:1-NAT)

Die im Folgenden aufgeführten Einstellungen sind auch nach dem Einbinden in eine Redundanzbeziehung für die einzelnen Security-Baugruppen aktiv. Diese Einstellungen können für beide Security-Baugruppen weiterhin separat angepasst werden.

- Schnittstellen-Einstellungen (Die Deaktivierung von Schnittstellen ist nicht möglich)
- Standardregeln für IP-Dienste (Firewall)

- DDNS
- Zeitsynchronisierung
- Log-Einstellungen
- SNMP
- MRP/HRP
- RADIUS

7.2 Redundanzbeziehungen anlegen und Security-Baugruppen zuordnen

Voraussetzungen

Es können nur Security-Baugruppen einer Redundanzbeziehung zugeordnet werden, die folgende Voraussetzungen erfüllen:

- Security-Baugruppe ist vom Typ "S623 V4" oder "S627-2M V4"
- Security-Baugruppe befindet sich im Routing-Modus
- Alle Schnittstellen der Security-Baugruppe sind aktiv
- IP-Zuweisungsmethode "Statische Adresse" ist für alle Schnittstellen projektiert
- Security-Baugruppe ist nicht Teilnehmer einer VPN-Gruppe
- Security-Baugruppe ist keiner anderen Redundanzbeziehung zugeordnet

Vorgehensweise

1. Wählen Sie im Navigationsbereich das Objekt "Redundanzbeziehungen".
2. Wählen Sie im Kontextmenü (rechte Maustaste) des Objekts den Menübefehl "Redundanzbeziehung einfügen...".

   Ergebnis: Die angelegte Redundanzbeziehung wird im Navigationsbereich angezeigt.

3. Ordnen Sie der Redundanzbeziehung die Security-Baugruppen zu, indem Sie diese im Inhaltsbereich selektieren und auf die angelegte Redundanzbeziehung im Navigationsbereich ziehen (Drag and Drop).
4. Im Dialog "Konfiguration der Redundanzbeziehung" haben Sie die folgenden Möglichkeiten zur Projektierung der Redundanzbeziehung:
   – Übernahme der Projektierung aus den Registern "Firewall", "Routing" sowie "NAT/NAPT" einer Security-Baugruppe für die Redundanzbeziehung. Aus der Klappliste können Sie die Security-Baugruppe auswählen, deren Projektierung Sie für die Redundanzbeziehung verwenden möchten. Eine bestehende Projektierung der Redundanzbeziehung wird dadurch überschrieben.
   – Erzeugen einer Kopie der zugeordneten Security-Baugruppe innerhalb der Redundanzbeziehung. Dies ist nur möglich, wenn nur eine Security-Baugruppe einer angelegten Redundanzbeziehung zugeordnet wird.

   Alternativ können Sie die Redundanzbeziehung nachträglich über die Eigenschaften der Redundanzbeziehung projektieren, siehe Kapitel:
   Redundanzbeziehungen konfigurieren (Seite 235)

Ergebnis: Sie haben eine Redundanzbeziehung angelegt und dieser die gewünschten Security-Baugruppen zugeordnet.

7.3 Redundanzbeziehungen konfigurieren

So erreichen Sie diese Funktion

Selektieren Sie im Navigationsbereich die Redundanzbeziehung und wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...".

Netzparameter der Redundanzbeziehung projektieren

Tabelle 7- 1 Parameter im Register "Grundeinstellungen"

Konfigurierbarer Parameter	Bedeutung
Primärbaugruppe	Auswahl der Security-Baugruppe, die im Normalbetrieb die aktive Security-Baugruppe sein soll.
Virtuelle Router-ID aktivieren (nur für SCALANCE S623/S627-2M ab Firmware V4.0.1)	Wenn Sie dieses Kontrollkästchen aktivieren, können Sie die virtuellen Router-IDs der virtuellen Schnittstellen anpassen. Über eine virtuelle Router-ID wird die virtuelle MAC-Adresse einer virtuellen Schnittstelle festgelegt. Mögliche Werte: 01...FF
IP-Adresse	Virtuelle IP-Adresse der externen bzw. internen Schnittstelle der Redundanzbeziehung
Subnetzmaske	Subnetzmaske der virtuellen externen bzw. internen Schnittstelle der Redundanzbeziehung

Konfigurierbarer Parameter	Bedeutung
Kommentar	Optionaler Kommentar
Virtuelle Router-ID (nur für SCALANCE S623/S627-2M ab Firmware V4.0.1)	Über eine virtuelle Router-ID wird die virtuelle MAC-Adresse einer virtuellen Schnittstelle festgelegt.

Für generelle Informationen zur Projektierung von Netzparametern, siehe folgendes Kapitel:
Baugruppen anlegen und Netzparameter einstellen (Seite 89)

Firewall projektieren

Die Projektierung von IP-Paketfilterregeln für Redundanzbeziehungen erfolgt nach dem gleichen Schema wie die Projektierung von IP-Paketfilterregeln für einzelne Security-Baugruppen. Zur Verfügung stehen die Kommunikationsrichtungen "Von Extern nach Intern" und " Von Intern nach Extern".

Für generelle Informationen zur Projektierung von IP-Paketfilterregeln im Erweiterten Modus, siehe folgende Kapitel:
IP-Paketfilter-Regeln (Seite 151)

Adressumsetzung mit NAT/NAPT projektieren

Die Projektierung von Adressumsetzung mit NAT/NAPT für die Redundanzbeziehung erfolgt nach dem gleichen Schema wie die Projektierung von Adressumsetzung mit NAT/NAPT für einzelne Security-Baugruppen. Für Redundanzbeziehungen kann ausschließlich Source-NAT und NAPT projektiert werden. Bei Source-NAT können Quell-IP-Adressen im internen Subnetz nur gegen die virtuelle externe IP-Adresse der Redundanzbeziehung ausgetauscht werden. Es können keine Alias-IP-Adressen an der externen Schnittstelle der Redundanzbeziehung registriert werden. Bei NAPT ist lediglich die Adressumsetzungsrichtung "Extern nach Intern" projektierbar.

Für generelle Informationen zur Projektierung von Adressumsetzungen mit NAT/NAPT, siehe folgendes Kapitel:
Adressumsetzung mit NAT/NAPT (Seite 175)

Routing projektieren

Die Projektierung von Routen für die Redundanzbeziehung erfolgt nach dem gleichen Schema wie die Projektierung von Routen für einzelne Security-Baugruppen.

Für generelle Informationen zur Projektierung von Routing, siehe folgendes Kapitel:
Standard-Router und Routen festlegen (Seite 172)

Siehe auch

MAC-Paketfilter-Regeln (Seite 161)

SOFTNET Security Client 8

Mit der PC-Software SOFTNET Security Client sind gesicherte Fernzugriffe vom PC/PG auf Automatisierungsgeräte, die durch Security-Baugruppen geschützt sind, über öffentliche Netze hinweg möglich.

In diesem Kapitel wird beschrieben, wie Sie den SOFTNET Security Client im Security Configuration Tool projektieren und anschließend auf dem PC/PG in Betrieb nehmen.

Weitere Informationen



Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe des SOFTNET Security Client.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

Siehe auch

Gesicherte Kommunikation im VPN über IPsec-Tunnel (Seite 201)

8.1 Einsatz des SOFTNET Security Client

Einsatzbereich - Zugriff über VPN

Mit dem SOFTNET Security Client konfigurieren Sie einen PC/PG so, dass er automatisch eine gesicherte IPsec-Tunnelverbindung im VPN (Virtual Private Network) zu einer oder mehreren Security-Baugruppen aufbauen kann.

PG/PC-Applikationen wie NCM Diagnose oder STEP 7 können über eine gesicherte Tunnelverbindung auf Geräte oder Netzwerke zugreifen, die sich in einem durch die Security-Baugruppe geschützten internen Netz befinden.

Fertigungsleitrechner
Workstation Computer
Exportieren der Konfiguration für SOFTNET Security Client mittels Datenträger
SOFTNET Security Client
Security-Baugruppe
Security-Baugruppe
Security-Baugruppe
IE/PB Link
ET 200X
S7-400
S7-300
OP 170
HMI
Automatisierungszelle
Automatisierungszelle

Automatische Kommunikation über VPN

Wichtig für Ihre Anwendung ist, dass der SOFTNET Security Client erkennt, wenn ein Zugriff auf die IP-Adresse eines VPN-Teilnehmers erfolgt. Adressieren Sie den Teilnehmer über die IP-Adresse so, als würde er sich im lokalen Subnetz befinden, an dem auch der PC/PG mit der Applikation angeschlossen ist.

Hinweis

Über den IPsec-Tunnel kann nur eine IP-basierte Kommunikation zwischen SSC und den Security-Baugruppen, sowie den internen Teilnehmern hinter den Security-Baugruppen erfolgen. Ebene2-Kommunikation ist mit dem SSC nicht möglich.

Bedienung



Die PC-Software SOFTNET Security Client dient zur Konfiguration der Security-Eigenschaften, welche zur Kommunikation mit durch Security-Baugruppen geschützten Geräten notwendig sind. Nach der Konfiguration läuft der SOFTNET Security Client im Hintergrund ab, sichtbar durch ein Symbol in der Symbolleiste auf dem PG/PC.

Details in der Online-Hilfe



Detaillierte Informationen zu den Dialogen und Eingabefeldern finden Sie auch in der Online-Hilfe der Bedienoberfläche des SOFTNET Security Client.

Sie erreichen die Online-Hilfe über die Schaltfläche "Hilfe" oder über die F1-Taste.

Wie funktioniert der SOFTNET Security Client?

Der SOFTNET Security Client liest die vom Projektierwerkzeug Security Configuration Tool erstellte Konfiguration ein und ermittelt ggf. aus der Datei die zu importierenden Zertifikate. Das Root-Certificate und die Private Keys werden importiert und im lokalen PG/PC abgelegt.

Anschließend werden mit den Daten aus der Konfiguration Security-Einstellungen vorgenommen, damit Applikationen über IP-Adressen auf Dienste auf und hinter den Security-Baugruppen zugreifen können.

Ist der Lernmodus für die internen Teilnehmer bzw. Automatisierungsgeräte aktiviert, stellt die Konfigurationsbaugruppe zunächst eine Sicherheitsrichtlinie für den gesicherten Zugriff auf die Security-Baugruppen ein. Danach ermittelt der SOFTNET Security Client die IP-Adressen der jeweils internen Teilnehmer und trägt diese in spezielle Filterlisten der Sicherheitsrichtlinie ein.

Ergebnis: Applikationen wie z. B. STEP 7 kommunizieren über VPN mit den Automatisierungsgeräten.

Hinweis

Auf einem Windows-System sind die IP-Sicherheitsrichtlinien benutzerspezifisch hinterlegt. Unter einem Benutzer kann jeweils nur eine IP-Sicherheitsrichtlinie gültig sein.

Wenn eine vorhandene IP-Sicherheitsrichtlinie nicht durch die Installation des SOFTNET Security Client überschrieben werden soll, nehmen Sie die Installation und Nutzung des SOFTNET Security Client unter einem speziell dafür eingerichteten Benutzer vor.

Unterstützte Betriebssysteme

Der SOFTNET Security Client ist für den Einsatz unter den folgenden Betriebssystemen geeignet:

- Microsoft Windows XP 32 Bit + Service Pack 3
- Microsoft Windows 7 Professional 32/64 Bit
- Microsoft Windows 7 Professional 32/64 Bit + Service Pack 1
- Microsoft Windows 7 Ultimate 32/64 Bit
- Microsoft Windows 7 Ultimate 32/64 Bit + Service Pack 1

Verhalten bei Störungen

Bei auftretenden Störungen auf Ihrem PG/PC verhält sich SOFTNET Security Client wie folgt:

- Eingerichtete Sicherheitsrichtlinien bleiben über das Aus- und Einschalten Ihres PG/PC erhalten;
- Bei fehlerhafter Konfiguration werden Meldungen ausgegeben.

8.2 Installation und Inbetriebnahme des SOFTNET Security Client

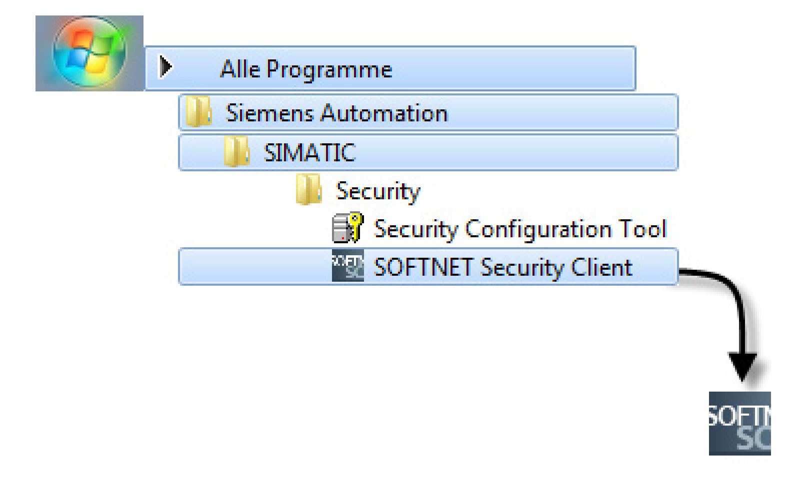
8.2.1 SOFTNET Security Client installieren und starten

Sie installieren die PC-Software SOFTNET Security Client von der Produkt DVD.

1. Lesen Sie zunächst die Angaben in der LIESMICH-Datei Ihrer SCALANCE S DVD und beachten Sie ggf. zusätzliche Installationshinweise.
2. Führen Sie das Setup-Programm aus;

   Öffnen Sie hierzu am einfachsten die Inhaltsübersicht Ihrer SCALANCE S DVD → wird beim DVD-Einlegen automatisch gestartet oder kann über die Datei start.exe geöffnet werden. Wählen Sie dann direkt den Eintrag "Installation SOFTNET Security Client"

Nach der Installation und dem Start des SOFTNET Security Client erscheint das Symbol für den SOFTNET Security Client in der Windows Taskleiste:



ACHTUNG
Inkompatibilität mit anderer VPN-Client-Software Wenn auf Ihrem PC neben dem SOFTNET Security Client weitere VPN-Client-Software installiert ist, können mit Hilfe des SOFTNET Security Clients unter Umständen keine VPN-Tunnel mehr aufgebaut werden. Deinstallieren Sie deshalb zunächst diese VPN-Client-Software, bevor Sie den SOFTNET Security Client verwenden.

SOFTNET Security Client einrichten

Einmal aktiviert, laufen die wichtigsten Funktionen im Hintergrund auf Ihrem PG/PC ab.

Die Projektierung des SOFTNET Security Client erfolgt folgendermaßen:

- Exportieren einer Security-Konfiguration aus dem Projektierwerkzeug Security Configuration Tool.
- Import der Security-Konfiguration in der eigenen Oberfläche, wie im nächsten Unterkapitel beschrieben.

Anlaufverhalten

Das Laden der Sicherheitsregeln kann einige Zeit in Anspruch nehmen. Die CPU des PG/PC wird in dieser Zeit bis zu 100% ausgelastet.

SOFTNET Security Client beenden

So beenden Sie den SOFTNET Security Client:

- Klicken Sie mit der rechten Maustaste auf das SOFTNET Security Client Symbol und wählen Sie die Option "Beende SOFTNET Security Client".
- Klicken Sie in der geöffneten Oberfläche auf die Schaltfläche "Beenden".

Ergebnis: Der SOFTNET Security Client wird beendet und die Sicherheitsrichtlinie deaktiviert.

8.2.2 SOFTNET Security Client deinstallieren

Bei der Deinstallation werden die vom SOFTNET Security Client eingestellten Security-Eigenschaften zurückgesetzt.

8.3 Konfigurationsdatei mit Projektierwerkzeug Security Configuration Tool erstellen

SOFTNET Security Client im SCT-Projekt konfigurieren

Der SOFTNET Security Client wird im SCT-Projekt als Baugruppe angelegt. Im Gegensatz zu den anderen Security-Baugruppen müssen Sie keine weiteren Eigenschaften projektieren.

Weisen Sie den angelegten SOFTNET Security Client der oder den VPN-Gruppen zu, in denen IPsec-Tunnel zum PG/PC eingerichtet werden sollen. Dabei werden die Gruppeneigenschaften übernommen, die Sie für diese VPN-Gruppen projektiert haben.

Hinweis

Beachten Sie die Angaben zu den Parametern in folgendem Kapitel:

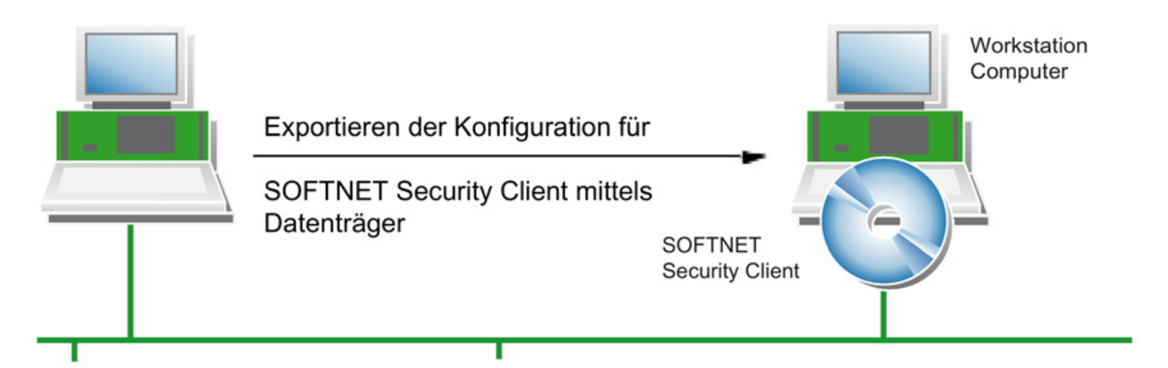
- Baugruppe in konfigurierte VPN-Gruppe aufnehmen (Seite 213)

Hinweis

Wenn Sie mehrere SOFTNET Security Clients innerhalb einer VPN-Gruppe anlegen, werden keine Tunnel zwischen diesen Clients aufgebaut, sondern nur vom jeweiligen Client zu den Security-Baugruppen.

Konfigurationsdateien für den SOFTNET Security Client

Die Schnittstelle zwischen dem Projektierwerkzeug Security Configuration Tool und dem SOFTNET Security Client wird über Konfigurationsdateien bedient.



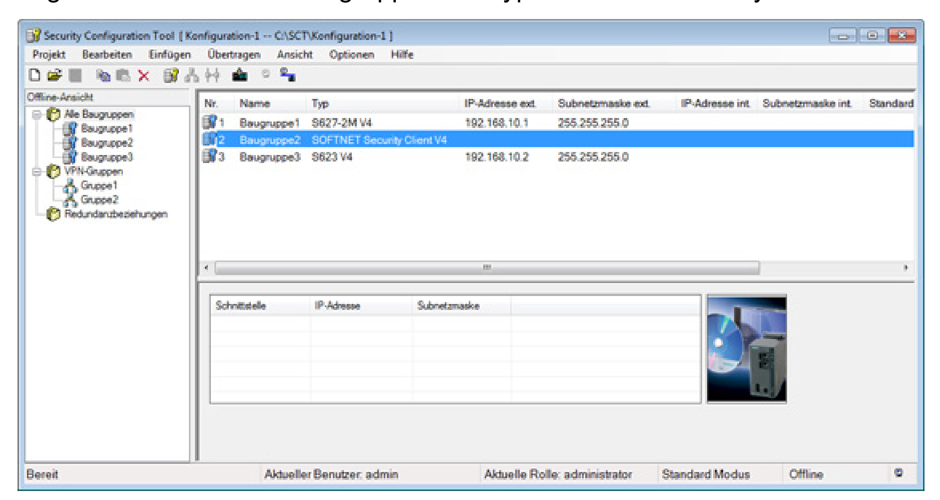
Die Konfiguration wird in folgenden Dateitypen hinterlegt:

- *.dat
- *.p12
- *.cer

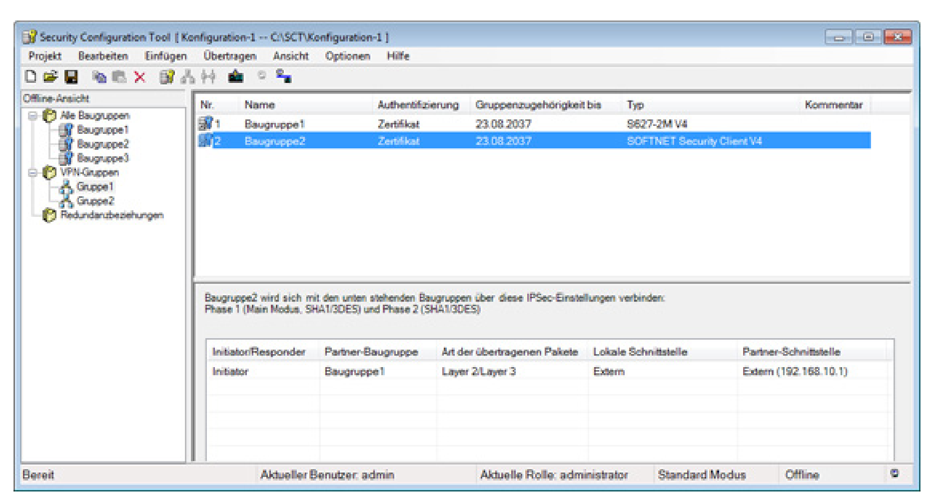
Vorgehensweise

Um die Konfigurationsdateien zu erzeugen, führen Sie in SCT folgende Schritte aus:

1. Legen Sie in SCT eine Baugruppe vom Typ SOFTNET Security Client an.



2. Ordnen Sie die SSC-Baugruppe den VPN-Gruppen zu, in denen der PG/PC über IPsec-Tunnel kommunizieren soll.



3. Wählen Sie den Menübefehl "Projekt" > "Speichern".
4. Selektieren Sie die Baugruppe vom Typ "SOFTNET Security Client" und wählen Sie den Menübefehl "Übertragen" > "An Baugruppe(n)...".
5. Wählen Sie den Speicherort für die Konfigurationsdateien.
6. Geben Sie im folgenden Dialog an, ob für das VPN-Gruppen-Zertifikat der Baugruppe ein eigenes Passwort erstellt werden soll.

   Wenn Sie "Nein" wählen, wird als Passwort der Projektname vergeben (z. B. SCALANCE_SSC_Konfiguration1), nicht das Projektpasswort.

   Wenn Sie "Ja" wählen (empfohlen), müssen Sie im darauf folgenden Dialog ein Passwort vergeben.
7. Übertragen Sie die Dateien vom Typ *.dat, *.p12, *.cer auf den PG/PC, auf dem Sie den SOFTNET Security Client betreiben möchten.

8.4 SOFTNET Security Client bedienen

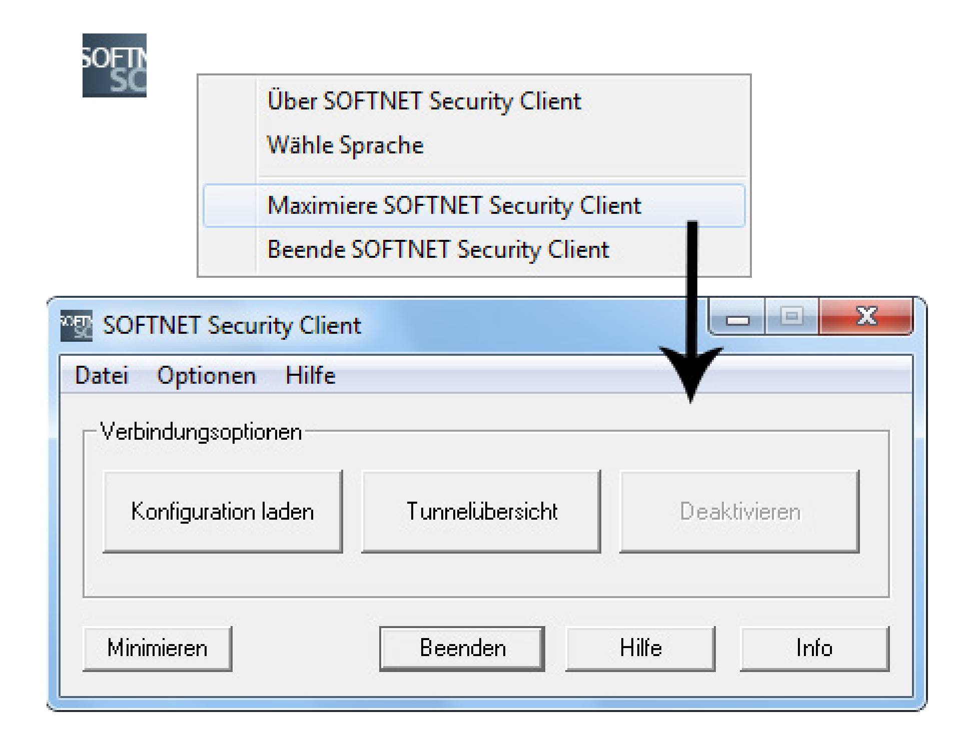
Konfigurierbare Eigenschaften

Im Einzelnen können Sie folgende Dienste nutzen:

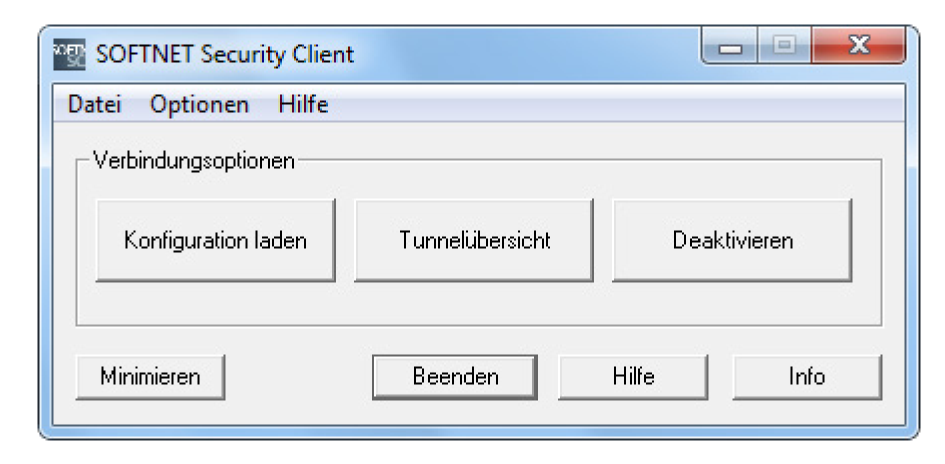
- Einrichten von sicherer IPsec-Tunnelkommunikation (VPN) zwischen dem PC/PG und allen Security-Baugruppen oder einzelnen Security-Baugruppen eines Projektes oder mehrerer Projekte. Über diese IPsec-Tunnel kann der PC/PG auf die Security-Baugruppe und die internen Knoten der Security-Baugruppe zugreifen.
- Aus- und Einschalten von bereits eingerichteten sicheren Verbindungen.
- Verbindungen bei nachträglich hinzugefügten Endgeräten einrichten. Dazu muss der Lernmodus aktiviert sein.
- Überprüfen einer Konfiguration, d. h. welche Verbindungen sind eingerichtet oder möglich.

So rufen Sie SOFTNET Security Client für die Konfiguration auf

Doppelklicken Sie auf das Symbol in der Windows Taskleiste oder wählen Sie über das Kontextmenü den Menüpunkt "Maximiere SOFTNET Security Client".



Über die Schaltflächen erreichen Sie folgende Funktionen:



Schaltfläche	Bedeutung
Konfiguration laden	Dialog zur Auswahl einer Konfigurationsdatei für den Import Wählen Sie eine Datei aus und klicken Sie auf die Schaltfläche "Öffnen". Ergebnis: Die Konfiguration wird eingelesen. Im Dialog wird abgefragt, ob die Tunnel für alle Security-Baugruppen sofort eingerichtet werden sollen. Für die in der Konfiguration eingetragenen IP-Adressen der Security-Baugruppen werden die Tunnel zu diesen IP-Adressen sofort eingerichtet. Diese Vorgehensweise ist besonders bei größeren Konfigurationen schnell und effizient. Optional können Sie im Dialog "Tunnelübersicht" alle Tunnel manuell über das Kontextmenü einrichten. Anmerkung: Sie können nacheinander die Konfigurationsdateien aus mehreren mit SCT erstellten Projekten importieren (siehe auch nachfolgende Erläuterung zur Vorgehensweise).
Tunnelübersicht	Dialog zum Einrichten und Bearbeiten sowie zum Diagnostizieren der Tunnel-Status Über diesen Dialog nehmen Sie die eigentliche Konfiguration des SOFTNET Security Client vor. Es wird eine Liste der gesicherten Tunnel mit den IP-Adressen der Security-Baugruppen angezeigt. Über die Icons jedes Listeneintrags können Sie die Tunnel-Status der jeweiligen Security-Baugruppen ermitteln. Über das Kontextmenü können Sie die Tunnel aktivieren / deaktivieren, testen sowie den Eintrag aus der Liste löschen. Falls auf Ihrem PG/PC mehrere Netzwerkadapter vorhanden sind, wählt der SOFTNET Security Client automatisch einen Netzwerkadapter aus, über den ein Tunnelaufbau versucht wird. Gegebenenfalls konnte der SOFTNET Security Client jedoch keinen zu Ihrem Teilnehmer passenden finden und hat einen beliebigen eingetragen. In diesem Fall müssen Sie die Netzwerkadaptereinstellung über den Dialog "Netzwerkadapter" manuell anpassen. Sie rufen diesen Dialog im Kontextmenü der Teilnehmer und Security-Baugruppen über den Eintrag "Wähle Netzwerkverbindung..." auf.
Deaktivieren	Alle gesicherten Tunnel werden deaktiviert.
Minimieren	Die Bedienoberfläche des SOFTNET Security Client wird geschlossen. Das Symbol für den SOFTNET Security Client wird weiterhin in der Windows Taskleiste angezeigt.
Beenden	Der SOFTNET Security Client wird beendet und alle Tunnel deaktiviert.

Schaltfläche	Bedeutung
Hilfe	Online-Hilfe aufrufen
Info	Informationen zum Ausgabestand des SOFTNET Security Client Details: Liste aller für die Funktion des SOFTNET Security Client benötigten Dateien mit Rückmeldung, ob diese auf dem System gefunden werden konnten.

8.5 Tunnel einrichten und bearbeiten

Einrichten von sicheren Verbindungen zu allen Security-Modulen

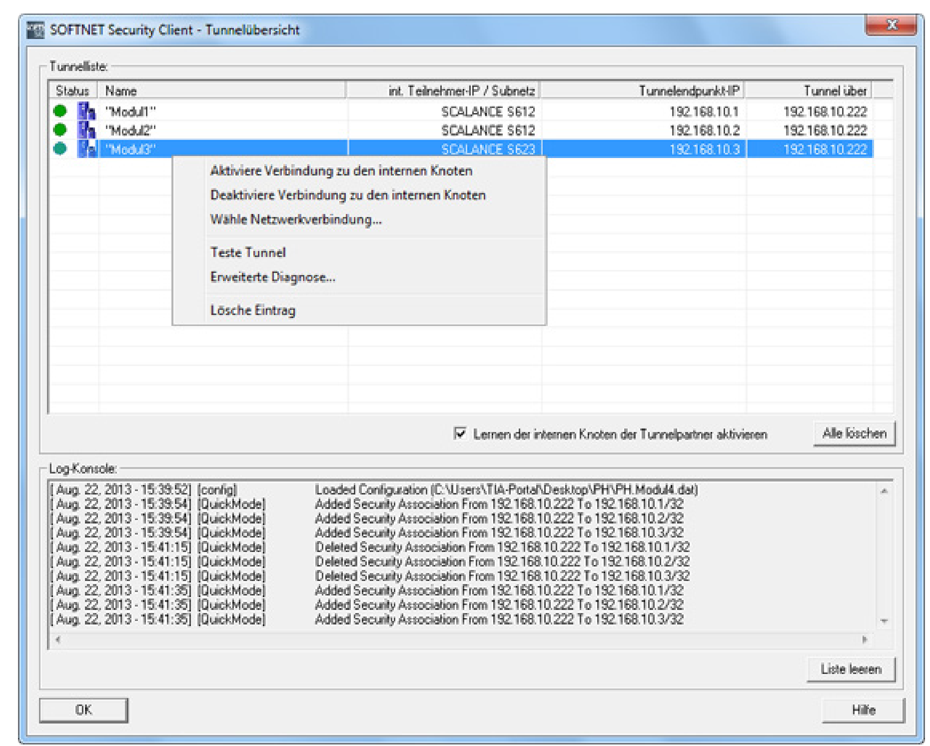
Im Dialog für den Konfigurationsimport wählen Sie, ob die Tunnelverbindung für alle internen Teilnehmer der Security-Baugruppe sofort eingerichtet werden sollen. Dadurch ergeben sich die folgenden Möglichkeiten:

- "Ja" - Tunnel automatisch aktivieren

  Für die in der Konfiguration eingetragenen IP-Adressen der Security-Baugruppen werden die Tunnel zu diesen IP-Adressen eingerichtet.

- "Nein" - Tunnelkonfiguration nur einlesen

  Optional können Sie die konfigurierten Tunnel nur einlesen und anschließend im Dialog "Tunnelübersicht" das Einrichten der Tunnel einzeln vornehmen.



So richten Sie die Tunnelverbindungen ein

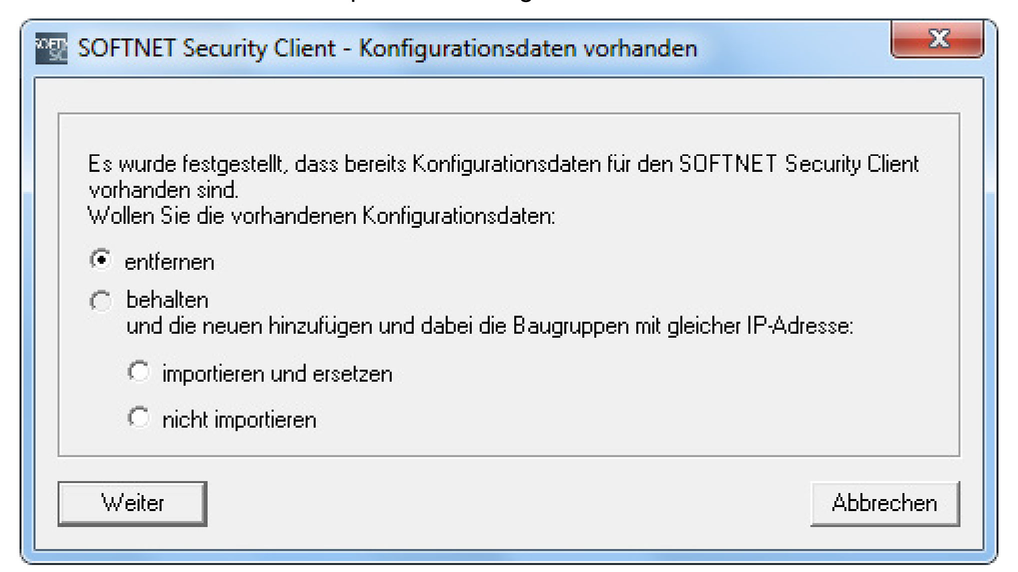
1. Öffnen Sie den Dialog zum Import der Konfigurationsdatei über die Schaltfläche "Konfiguration laden".
2. Wählen Sie die mit SCT erstellte Konfigurationsdatei aus (Dateiformat ".dat").

   Sie können Konfigurationsdaten aus mehreren Projekten gleichzeitig einlesen. Falls im SOFTNET Security Client bereits Konfigurationsdaten vorliegen, wählen Sie eine der folgenden Optionen aus:

   – "entfernen": Nur die zuletzt geladenen Konfigurationsdaten sind verfügbar.

   – "importieren und ersetzen": Ist bei geänderten Konfigurationsdaten sinnvoll, beispielsweise nur die Konfiguration im Projekt a ist geändert, die Konfigurationsdaten von Projekt b und c bleiben unverändert erhalten und die geänderten Konfigurationsdaten werden in Projekt a ersetzt.

   – "nicht importieren": ist sinnvoll, wenn in einem Projekt eine Security-Baugruppe hinzugefügt wurde. Die bestehende SSC-Konfiguration mit bereits importierten Security-Baugruppen wird nicht verändert, gelernte interne Knoten dieser Baugruppen würden bei einer anderen Option verloren gehen.

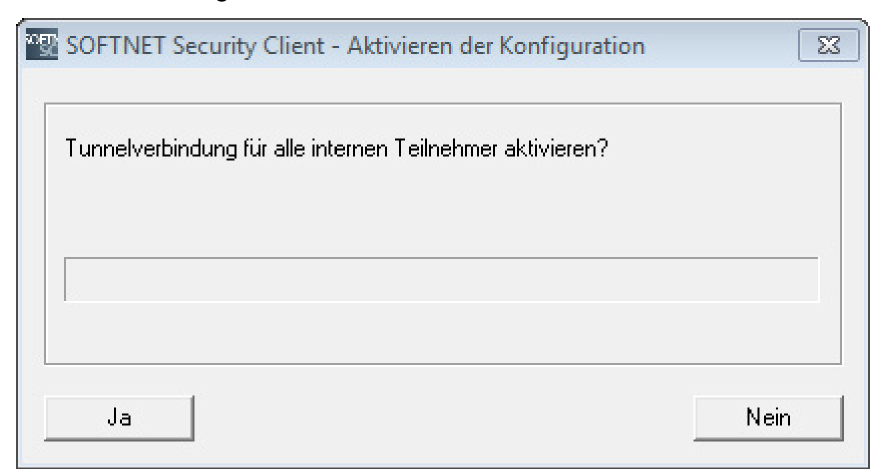


3. Wenn Sie in SCT als Authentifizierungsmethode "Zertifikat" gewählt haben, geben Sie ein Passwort für das Zertifikat der VPN-Konfiguration an. Haben Sie kein Passwort im SCT vergeben, wurde der Projektname (nicht das Projektpasswort des eingeloggten Benutzers) als Passwort übernommen.
4. Falls Sie bei der Konfiguration im Security Configuration Tool eine SCALANCE M875 Baugruppe, SCALANCE M-800 Baugruppe oder einen S7-CP mit aktiviertem DHCP an der GBit-Schnittstelle projektiert haben, erscheint der Dialog "IP-/DNS-Einstellungen". Gehen Sie abhängig vom projektierten Baugruppentyp folgendermaßen vor:

   – Für SCALANCE M875 Baugruppen und SCALANCE M-800 Baugruppen: Wählen Sie, ob Sie den Tunnel zur Baugruppe über die vom ISP zur Laufzeit bezogene IP-Adresse oder alternativ über einen DNS-Namen aufbauen wollen.

   – Für S7-CPs mit aktiviertem DHCP an der GBit-Schnittstelle: Geben Sie die über DHCP zugewiesene IP-Adresse ein.

5. Wählen Sie aus, ob für die internen Teilnehmer der Security-Baugruppe die Tunnelverbindungen aktiviert werden sollen.



   Falls Sie die Aktivierung hier noch nicht anstoßen, können Sie dies jederzeit im nachfolgend beschriebenen Dialog "Tunnelübersicht" durchführen.

   Wenn Sie die Aktivierung der Tunnelverbindungen gewählt haben, werden nun die Tunnelverbindungen zwischen dem SOFTNET Security Client und den Security-Baugruppen aufgebaut.

   Dies kann einige Zeit in Anspruch nehmen.

6. Öffnen Sie den Dialog "Tunnelübersicht".

   In der Tabelle werden die Security-Baugruppen und internen Teilnehmer mit Statusinformationen zu den Tunnelverbindungen angezeigt.

7. Falls Knoten bzw. Teilnehmer in der Tabelle nicht angezeigt werden, setzen Sie über die Kommandozeile ein Ping-Kommando an den fehlenden Knoten ab.

   Ergebnis: Der Knoten wird von der Security-Baugruppe gelernt und an den SOFTNET Security Client weitergegeben. Wird er dennoch nicht gelernt, sollten Sie den Knoten bzw. Teilnehmer statisch im VPN-Register konfigurieren.

   Anmerkung:

   Falls der Dialog nicht geöffnet ist während ein Teilnehmer erfasst wird, wird der Dialog automatisch aufgeblendet. Diese Funktion kann unter "Optionen" > "Einstellungen..." deaktiviert werden.

Hinweis

Statisch konfigurierte Teilnehmer und Subnetze

Wenn Sie Teilnehmer oder Subnetze nachträglich statisch konfigurieren, müssen Sie auch die Konfiguration für einen in der VPN-Gruppe genutzten SOFTNET Security Client neu laden.

---

8. Aktivieren Sie die Teilnehmer, bei denen noch keine Tunnelverbindung aufgebaut ist.

   Nach erfolgreichem Verbindungsaufbau starten Sie die Applikation, die eine Kommunikationsverbindung zu einem der Teilnehmer aufbauen soll, z. B. STEP 7.

Hinweis

Wenn auf dem PG/PC mehrere Netzwerkadapter vorhanden sind, wählt SSC den Netzwerkadapter zum Aufbau eines Tunnels automatisch aus. Dies kann unter Umständen nicht der gewünschte Netzwerkadapter sein. Falls kein zum Projekt passender Netzwerkadapter vorhanden ist, trägt SSC automatisch einen ein. Passen Sie in diesem Fall die Einstellung zum Netzwerkadapter über das Kontextmenü der Teilnehmer und Security-Baugruppen im Dialog "Tunnelübersicht" an.

Bedeutung der Parameter

Tabelle 8- 1 Parameter im Dialogfeld "Tunnelübersicht"

Parameter	Bedeutung / Wertebereich
Status	Die Bedeutung der Statusanzeigen finden Sie in der nachfolgenden Tabelle.
Name	Aus der SCT-Konfiguration übernommener Name der Baugruppe oder des Teilnehmers.
Int. Teilnehmer-IP / Subnetz	Wenn interne Teilnehmer / Subnetze vorhanden sind, wird die IP-Adresse des internen Knotens bzw. die Netz-ID des internen Subnetzes anzeigt.
Tunnelendpunkt-IP	IP-Adresse der zugeordneten Security-Baugruppe.
Tunnel über…	Falls der PC mit mehreren Netzwerkkarten betrieben wird, wird die zugeordnete IP-Adresse angezeigt, über welche der VPN-Tunnel aufgebaut wird.

Tabelle 8- 2 Statusanzeigen*

Symbol	Bedeutung
	Es besteht keine Verbindung zur Security-Baugruppe oder zum Teilnehmer.
	Es sind weitere Teilnehmer vorhanden, die nicht angezeigt werden. Doppelklicken Sie auf das Symbol, um weitere Teilnehmer anzuzeigen.
	Tunnel zu Teilnehmer ist deaktiviert. Es ist keine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren unverschlüsselt zu diesem Teilnehmer.
	Tunnel zu Teilnehmer ist aktiviert. Es ist eine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren verschlüsselt und damit sicher zu diesem Teilnehmer.
	Tunnel zu SCALANCE S-Baugruppe ist deaktiviert. Es ist keine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren unverschlüsselt zu dieser Security-Baugruppe.
	Tunnel zu SCALANCE S-Baugruppe ist aktiviert. Es ist eine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren verschlüsselt und damit sicher zu dieser Security-Baugruppe.
	Tunnel zu SCALANCE M Baugruppe ist deaktiviert. Es ist keine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren unverschlüsselt zu dieser Security-Baugruppe.
	Tunnel zu SCALANCE M Baugruppe ist aktiviert. Es ist eine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren verschlüsselt und damit sicher zu dieser Security-Baugruppe.
	Tunnel zu CP343-1 Advanced ist deaktiviert. Es ist keine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren unverschlüsselt zu diesem CP.
	Tunnel zu CP343-1 Advanced ist aktiviert. Es ist eine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren verschlüsselt und damit sicher zu diesem CP.
	Tunnel zu CP443-1 Advanced ist deaktiviert. Es ist keine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren unverschlüsselt zu diesem CP.
	Tunnel zu CP443-1 Advanced ist aktiviert. Es ist eine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren verschlüsselt und damit sicher zu diesem CP.
	Tunnel zu CP1628 ist deaktiviert. Es ist keine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren unverschlüsselt zu diesem CP.
	Tunnel zu CP1628 ist aktiviert. Es ist eine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren verschlüsselt und damit sicher zu diesem CP.
	Tunnel zu internem Subnetz ist deaktiviert. Es ist keine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren unverschlüsselt zu diesem Subnetz.
	Tunnel zu internem Subnetz ist aktiviert. Es ist eine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren verschlüsselt und damit sicher zu diesem Subnetz.
	Baugruppe / Teilnehmer ist nicht erreichbar.
	Baugruppe / Teilnehmer ist erreichbar, Tunnel zu Baugruppe / Teilnehmer ist jedoch deaktiviert. Es ist keine IP-Sicherheitsrichtlinie im System eingerichtet. Sie kommunizieren unverschlüsselt zu dieser Baugruppe / zu diesem Teilnehmer.
	Baugruppe / Teilnehmer ist erreichbar, Tunnel zu Baugruppe / Teilnehmer ist aktiviert.
	Erreichbarkeitstest deaktiviert. Es kann keine Aussage über die Erreichbarkeit der Baugruppe / des Teilnehmers getroffen werden.

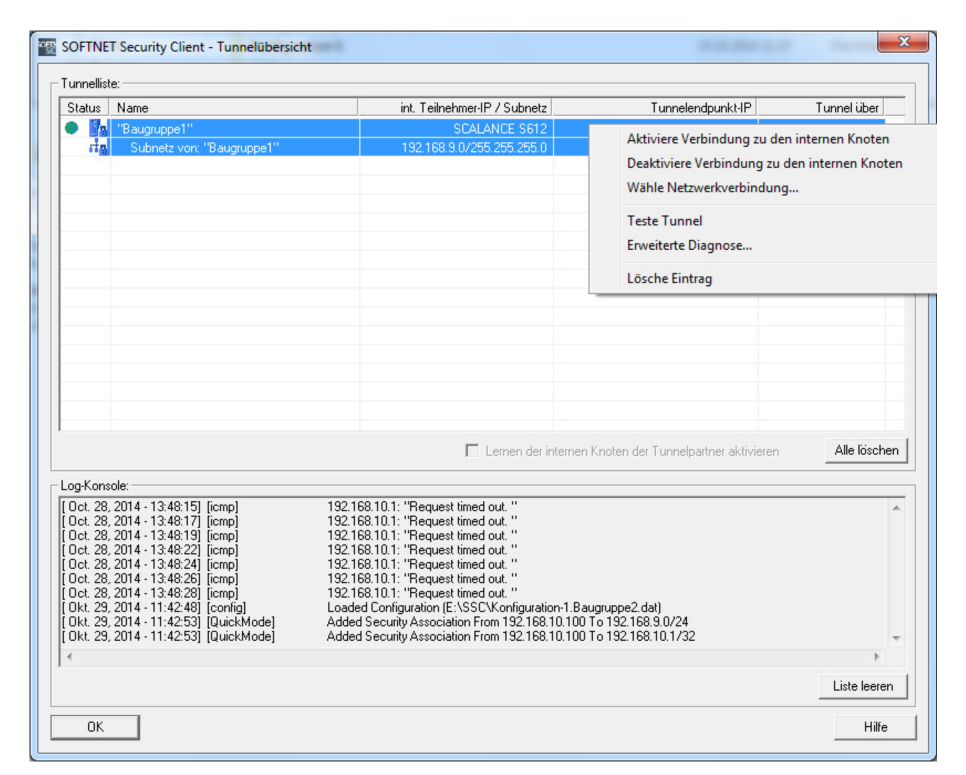
* Die Tabelle ist gültig für Windows XP. Unter Windows 7 ist die Tabelle bei aktivierter Windows-Firewall gültig.

Bedienelemente des Dialogs "Tunnelübersicht"

Bedienelement	Bedeutung
Optionskästchen "Lernen der internen Knoten der Tunnelpartner aktivieren"	Ist in der Konfiguration der Security-Baugruppen der Lernmodus aktiviert, kann dieser auch für den SOFTNET Security Client aktiviert werden. Dadurch erhalten Sie automatisch die Informationen über die internen Teilnehmer der Security-Baugruppen in der Tunnelübersicht. Ansonsten ist das Auswahlfeld "Lernen der internen Knoten" inaktiv und es werden keine Informationen über die internen Teilnehmer der Security-Baugruppen in der Tunnelübersicht dargestellt.
Schaltfläche "Alle löschen"	Die IP-Sicherheitsrichtlinien der in SSC eingerichteten Einträge werden gelöscht.
Schaltfläche "Liste leeren"	Löscht alle Einträge in der Log-Konsole.

Tunnel-Eintrag selektieren und bedienen - Optionen des Kontextmenüs

Wählen Sie im Dialog "Tunnelübersicht" einen Eintrag aus und öffnen Sie über das Kontextmenü weitere Optionen.



Menübefehl	Bedeutung
Aktiviere Verbindung zu den internen Knoten / Deaktiviere Verbindung zu den internen Knoten	Eingerichtete sichere Verbindungen schalten Sie über den Eintrag "Deaktiviere Verbindung zu den internen Knoten" aus. Ergebnis: Auf dem PC wird die Security Policy deaktiviert. Um die Änderung rückgängig zu machen und die Tunnel wieder zu aktivieren, klicken Sie auf den Eintrag "Aktiviere Verbindung zu den internen Knoten".
Wähle Netzwerkverbindung...	Für jede Security-Baugruppe können Sie über den Menübefehl "Wähle Netzwerkverbindung..." des Kontextmenüs einen Netzwerkadapter auswählen, über welchen der Tunnel eingerichtet werden soll.
Teste Tunnel	Testen der Tunnelverbindung.
Erweiterte Diagnose...	Ruft den Dialog "Erweiterte Moduldiagnose" auf.
IP-Adresse/DNS-Name ändern (nur für SCALANCE M)	Ändern der IP-Adresse bzw. des DNS-Namens des selektierten Eintrags.
Lösche Eintrag	Die IP-Sicherheitsrichtlinie des selektierten Eintrags wird gelöscht.

Hinweis

Erweiterung der Policy bei Aktivierung interner Teilnehmer

Bitte beachten Sie, dass beim einzelnen Aktivieren der internen Teilnehmer die Policy im System jeweils erweitert wird. Ein Deaktivieren des Gesamtsystems (über das Kontextmenü des übergeordneten SCALANCE S) führt jedoch nicht zur Anpassung der Policy, sondern nur zu deren Deaktivierung. Somit wird bei der Aktivierung eines internen Teilnehmers immer die deaktivierte Gesamtpolicy plus dem zusätzlichen internen Teilnehmer aktiviert. Wenn Sie sicher sein wollen, dass die eingerichtete Policy sich vollständig auf die von Ihnen aktivierten Teilnehmer bezieht, schließen Sie den SOFTNET Security Client und öffnen Sie ihn erneut.

Erweiterte Moduldiagnose

Um die erweiterte Moduldiagnose aufzurufen, wählen Sie den Menübefehl "Erweiterte Diagnose..." im Kontextmenü eines Eintrags. Alternativ können Sie den Dialog über den Menübefehl "Optionen" > "Erweiterte Moduldiagnose" im Hauptfenster des SOFTNET Security Clients aufrufen.

Die Ansicht dient nur der Diagnose des Systemzustandes im Zusammenhang mit den konfigurierten Security-Baugruppen und kann bei Anfragen beim Customer Support helfen.

- SCALANCE S / MD74x Modul / CP

  Hier wählen Sie die Security-Baugruppe aus, für die der aktuelle Systemstatus diagnostiziert werden soll.

  Anmerkung: Sämtliche Security-Baugruppen, die über die Konfiguration eingelesen wurden, sind auswählbar.

- Routingeinstellungen (Modulspezifische Parameter)

  Zeigt die aus der Konfiguration ermittelten Einstellungen zu Schnittstellen und internen Knoten/Subnetzen an.

- Aktive Main Modes / Aktive Quick Modes

  Sind für die ausgewählte Baugruppe auf dem PG/PC Main Modes bzw. Quick Modes eingerichtet, werden die dazugehörigen Details hier angezeigt. Dazu gehört auch die gesamte Anzahl der Main Modes bzw. Quick Modes, die zu der ausgewählten Baugruppe auf dem System gefunden wurden.

- Routingeinstellungen (Netzwerkeinstellungen des Rechners)

  Zeigt die aktuellen Routing-Einstellungen des Rechners an.

  Über die Option "Alle Routingeinstellungen anzeigen" erhalten Sie zusätzliche Routing-Angaben.

- Zugewiesene IP-Adressen

  Liste über die dem Rechner bekannten Netzwerkschnittstellen in Verbindung mit den konfigurierten bzw. zugewiesenen IP-Adressen.

Log-Konsole

Welche Einträge in der Log-Konsole angezeigt werden, wählen Sie im Dialog "Einstellungen" aus. Sie erreichen diesen im Hauptdialog des SOFTNET Security Clients über den Menübefehl "Optionen" > "Einstellungen...".

Folgende Informationen werden angezeigt:

- Diagnoseinformationen zum Verbindungsaufbau mit den konfigurierten Security-Baugruppen und internen Teilnehmern / Subnetzen.
- Datums- und Zeitstempel zum Zeitpunkt der Ereignisse
- Auf- und Abbau einer Security Association
- Negativ verlaufener Erreichbarkeitstest (Test-Ping) zu den konfigurierten Teilnehmern
- Laden von Konfigurationsdateien
- Lernen/Verlernen interner Teilnehmer/Subnetze

Globale Einstellungen für den SOFTNET Security Client

1. Öffnen Sie im Hauptdialog des SOFTNET Security Clients den Menüpunkt "Optionen" > "Einstellungen".
2. Nehmen Sie globale Einstellungen vor, die nach dem Beenden und Öffnen des SOFTNET Security Client erhalten bleiben.

Die Funktionen entnehmen Sie aus der folgenden Tabelle.

Funktion	Beschreibung / Optionen
Logfile Größe	Größe der Datei, welche die Meldungen enthält, die in der Log-Konsole der Tunnelübersicht ausgegeben werden. Da die Log-Daten über Umlaufpuffer in der Datei gespeichert werden, wählen Sie über die Größe der Datei aus, wie lange die Log-Daten in der Datei gespeichert bleiben.
Anzahl anzuzeigender Meldungen in Log-Konsole der Tunnelübersicht	Anzahl der Meldungen, welche aus dem Logfile extrahiert und in der Log-Konsole der Tunnelübersicht angezeigt werden.
Folgende Log-Meldungen in Log-Konsole der Tunnelübersicht ausgeben: • Anzeige des negativen Erreichbarkeitstest (Ping) • Anlegen / Löschen von Security Associations (Quick Modes) • Anlegen / Löschen von Main Modes • Laden von Konfigurationsdateien • Lernen interner Teilnehmer	Auswahl, welche Arten von Meldungen in der Log-Konsole der Tunnelübersicht angezeigt werden.
Logfile-Größe (Debug-Logfiles)	Logfile-Größe der Quelldateien für Debug-Meldungen des SOFTNET Security Client (können vom Customer Support angefordert werden, um Analysen zu erleichtern)
Erreichbarkeitstest, Wartezeit auf Rückantwort	Einstellbare Wartezeit für den Ping, welcher die Erreichbarkeit eines Tunnelpartners angeben soll. Vor allem einzustellen bei Tunneln mit langsamen Übertragungswegen (UMTS, GPRS, etc.), bei denen die Laufzeit der Datenpakete deutlich erhöht ist. Beeinflusst somit direkt die Anzeige der Erreichbarkeit in der Tunnelübersicht.

Funktion	Beschreibung / Optionen
Erreichbarkeitstest global deaktivieren	Wenn Sie diese Funktion aktivieren, wird der Erreichbarkeitstest global für alle enthaltenen Konfigurationen im SOFTNET Security Client deaktiviert. Vorteil: Es wird kein zusätzliches Datenvolumen erzeugt. Nachteil: Sie erhalten in der Tunnelübersicht keine Rückmeldung, ob ein Tunnelpartner erreichbar ist oder nicht.
Tunnelübersicht-Fenster bei Änderung eines gelernten Teilnehmers im Vordergrund zeigen	Wenn Sie diese Funktion aktivieren, wird der Dialog "Tunnelübersicht" automatisch aufgeblendet, wenn ein neuer interner Teilnehmer erkannt wurde.

Online-Funktionen - Diagnose und Logging 9

Zu Test- und Überwachungszwecken verfügt die Security-Baugruppe über Diagnose- und Logging-Funktionen.

- Diagnosefunktionen

  Hierunter sind verschiedene System- und Statusfunktionen zu verstehen, die Sie im Online-Modus anwenden können.

- Logging-Funktionen

  Hierbei geht es um die Aufzeichnung von System- und Sicherheitsereignissen.

Die Aufzeichnung der Ereignisse erfolgt in Pufferbereiche der Security-Baugruppe oder auf einem Syslog-Server. Die Parametrierung und Auswertung dieser Funktionen setzt eine Netzwerkverbindung auf die ausgewählte Security-Baugruppe voraus.

Ereignisse mit Logging-Funktionen aufzeichnen

Welche Ereignisse aufgezeichnet werden sollen, legen Sie mit den Log-Einstellungen zur jeweiligen Security-Baugruppe fest.

Dabei können Sie für die Aufzeichnung folgende Varianten konfigurieren:

- Lokales Logging

  Bei dieser Variante zeichnen Sie die Ereignisse in lokalen Puffern der Security-Baugruppe auf. Im Online-Dialog des Security Configuration Tool können Sie dann auf diese Aufzeichnungen zugreifen, diese sichtbar machen und in der Service-Station archivieren.

- Netzwerk Syslog

  Beim Netzwerk Syslog nutzen Sie einen im Netz vorhandenen Syslog-Server, an den die Ereignisse gesendet werden. Welche Ereignisse gesendet werden, geben Sie in den Log-Einstellungen der jeweiligen Security-Baugruppe an.

Log-Daten archivieren und aus Datei einlesen

Sie können die aufgezeichneten Ereignisse zur Archivierung in einer Log-Datei speichern und diese im Offline-Modus öffnen. Wählen Sie hierzu den Menübefehl "Optionen" > "Log-Dateien..." und selektieren Sie über die Schaltfläche "Öffnen..." die zu öffnende Log-Datei. Weitere Informationen finden Sie in folgendem Kapitel:

- Funktionsübersicht Online-Dialog (Seite 259)

Diagnose im Ghost-Modus S602 ≥V3.1

Nach dem Bezug einer IP-Adresse vom internen Teilnehmer besitzt die Security-Baugruppe an der externen Schnittstelle eine IP-Adresse, die von derjenigen IP-Adresse abweichen kann, mit welcher die Security-Baugruppe initial projektiert wurde. Bevor Sie eine Diagnose über die externe Schnittstelle durchführen können, müssen Sie im Security Configuration Tool für die externe Schnittstelle die initial projektierte IP-Adresse durch diejenige ersetzen, die die Security-Baugruppe zur Laufzeit vom internen Teilnehmer bezogen hat.

Exportierte Log-Dateien vor unberechtigtem Zugriff schützen

Aus dem Security Configuration Tool exportierte Log-Dateien können sicherheitsrelevante Informationen enthalten. Stellen Sie deshalb sicher, dass diese Dateien vor unberechtigtem Zugriff geschützt sind. Dies ist insbesondere bei der Weitergabe der Dateien zu beachten.

9.1 Funktionsübersicht Online-Dialog

Die Security-Baugruppe bietet im Security Configuration Tool folgende Funktionen im Online-Dialog:

Tabelle 9- 1 Funktionen und Logging in der Online-Diagnose

Funktion / Register im Online-Dialog		Bedeutung
System- und Statusfunktionen		
	Zustand	Anzeige des Geräte-Status der im Projekt angewählten Security-Baugruppe.
SCA. S	Datum und Uhrzeit	Einstellung von Datum und Uhrzeit.
S≥V3.0	Schnittstellen-Einstellungen	Übersicht zu den Einstellungen der einzelnen Schnittstellen.
S≥V3.0	Dynamisches DNS	Übersicht zu den Einstellungen für dynamisches DNS
S≥V3.0	ARP-Tabelle	Anzeige der ARP-Tabelle der Security-Baugruppe.
S≥V3.0	Angemeldete Benutzer	Anzeige der Benutzer, die an der Internetseite für benutzerspezifische IP-Regelsätze angemeldet sind.
~~S602~~	Kommunikationszustand	Anzeige des Kommunikationszustands und der internen Netzknoten von Security-Baugruppen, die sich in derselben VPN-Gruppe befinden wie die ausgewählte Security-Baugruppe.
~~S602~~ ~~PC-CP~~	Interne Knoten	Anzeige der internen Netzknoten der Security-Baugruppe.
S7-CP	Dynamisch aktualisierte Firewall-Regeln	Anzeige der IP-Adressen, die über HTTP oder HTTPS dynamisch freigeschaltet oder von einem Benutzer nachgeladen wurden. Eine Aktualisierung der IP-Adressen in diesem Register kann durch folgende Ereignisse erfolgen: • Erweiterung/Veränderung der IP Access Control-Liste • Aktualisierung der Firewall-Regeln • Dynamische Erweiterungen, die vom CP zur Laufzeit eingetragen werden, z.B. PROFINET IO-Devices Da in diesem Register nur die dynamisch aktualisierten Firewall-Regeln angezeigt werden, müssen in eine vollständige Betrachtung des aktuellen Firewall-Zustands der Baugruppe auch diejenigen Firewall-Regeln einbezogen werden, die offline projektiert wurden.
S602 ≥V3.1	Ghost-Modus	Dialog für den Ghost-Modus des SCALANCE S602 mit Informationen zur IP-Adresse des internen Teilnehmers (identisch zur externen IP-Adresse der Security-Baugruppe) und zu IP-Adresswechseln am internen Teilnehmer.
S≥V4.0	IP-Blacklist	Anzeige der IP-Adressen, die in die Blacklist der Firewall eingetragen wurden.
Logging-Funktionen		

Funktion / Register im Online-Dialog		Bedeutung
	System-Log	Anzeige von geloggten System-Ereignissen sowie Starten und Stoppen der Anzeige.
	Audit-Log	Anzeige von geloggten Sicherheits-Ereignissen sowie Starten und Stoppen der Anzeige.
	Paketfilter-Log	Anzeige von geloggten Daten-Paketen sowie Starten und Stoppen der Anzeige.



Nähere Informationen zu den Einstellmöglichkeiten in den einzelnen Registern erhalten Sie in der Online-Hilfe.

Zugriffsvoraussetzungen

Damit Sie an einer Security-Baugruppe die Online-Funktionen nutzen können, müssen folgende Voraussetzungen erfüllt sein:

- eine Netzwerkverbindung zur ausgewählten Baugruppe besteht
- das Projekt, mit dem die Baugruppe konfiguriert wurde, ist geöffnet
- die Online-Betriebsart im Security Configuration Tool ist aktiv oder die baugruppenspezifische Online-Diagnose wurde über das Kontextmenü geöffnet.
- Für CPs muss der Diagnosezugang in der Firewall freigegeben sein (TCP 443)

Hinweis

Voraussetzung für die Online-Diagnose im Ghost-Modus 

Die Online-Diagnose ist im Ghost-Modus erst dann verfügbar, wenn die Security-Baugruppe die IP-Adresse des internen Teilnehmers gelernt und für ihre externe Schnittstelle übernommen hat. Danach ist die Security-Baugruppe über die IP-Adresse der externen Schnittstelle erreichbar.

Warnmeldung bei nicht aktueller Konfiguration oder Fremdprojekt

Wenn Sie den Online-Dialog aufrufen, wird geprüft, ob die aktuelle Konfiguration auf der Security-Baugruppe und die Konfiguration des geladenen Projekts übereinstimmen. Unterscheiden sich die beiden Konfigurationen, so wird eine Warnmeldung ausgegeben. Dadurch wird signalisiert, dass Sie entweder die Konfiguration (noch) nicht aktualisiert haben, oder das falsche Projekt verwenden.

Anzeige des Aufzeichnungszustands

Der aktuelle Aufzeichnungszustand ergibt sich aus der geladenen Konfiguration oder aus der Umkonfiguration im Online-Dialog. Mögliche Puffer-Einstellungen sind Umlaufspeicher oder Linearer Speicher. Welche Einstellung gerade aktiv ist, können Sie folgendermaßen ermitteln:

1. Wechseln Sie über den Menübefehl "Ansicht" > "Online" die Betriebsart.
2. Markieren Sie die zu bearbeitende Security-Baugruppe.
3. Wählen Sie den Menübefehl "Bearbeiten" > "Online-Diagnose...".

   Sobald Sie eines der Register für Log-Funktionen öffnen, sehen Sie im unteren Bereich des Registers den aktuellen Zustand der Puffer-Einstellung der gewählten Security-Baugruppe

Online-Einstellungen werden nicht in der Konfiguration gespeichert

Einstellungen, die Sie in der Online-Betriebsart vornehmen (z. B. Puffer-Einstellungen bei Log-Funktionen), werden nicht in der Konfiguration auf der Security-Baugruppe gespeichert. Nach einem Baugruppen-Neuanlauf sind deshalb immer die Einstellungen aus der Offline-Konfiguration wirksam.

9.2 Ereignisse aufzeichnen (Logging)

Übersicht

Ereignisse auf der Security-Baugruppe können aufgezeichnet werden. Die Aufzeichnung erfolgt je nach Ereignistyp in flüchtige oder dauerhafte lokale Pufferbereiche. Alternativ kann auch eine Aufzeichnung in einem Netzwerk-Server erfolgen.

Konfiguration im Standard Modus und im Erweiterten Modus

Die Auswahlmöglichkeiten im Security Configuration Tool hängen von der gewählten Ansicht ab:

- Standard Modus

  "Lokales Logging" ist im Standard Modus standardmäßig aktiviert; Paketfilter-Ereignisse können global im Register "Firewall" aktiviert werden. "Netzwerk Syslog" ist in dieser Ansicht nicht möglich.

- Erweiterter Modus

  Sämtliche Logging-Funktionen können im Register "Log-Einstellungen" einer selektierten Baugruppe aktiviert oder deaktiviert werden; Paketfilter-Ereignisse müssen zusätzlich selektiv im Register "Firewall" (lokale oder globale Regeln) aktiviert werden.

Aufzeichnungsverfahren und Ereignisklassen

Sie können in der Konfiguration festlegen, welche Daten aufgezeichnet werden sollen. Dadurch aktivieren Sie die Aufzeichnung bereits mit dem Laden der Konfiguration auf die Security-Baugruppe.

Außerdem wählen Sie in der Konfiguration eine oder beide der möglichen Aufzeichnungsverfahren:

- Lokales Logging
- Netzwerk Syslog

Die Security-Baugruppe kennt für beide Aufzeichnungsverfahren die folgenden Ereignisse:

Funktion	Funktionsweise
Paketfilter-Ereignisse (Firewall)	Der Paketfilter-Log zeichnet bestimmte Pakete des Datenverkehrs auf. Es werden nur Datenpakete geloggt, auf die eine projektierte Paketfilter-Regel (Firewall) zutrifft, oder auf die der Basisschutz reagiert (korrupte bzw. ungültige Pakete). Voraussetzung ist, dass die Aufzeichnung für die Paketfilter-Regel aktiviert ist.
Audit-Ereignisse	Der Audit-Log zeichnet automatisch fortlaufend sicherheitsrelevante Ereignisse auf, wie z. B. Benutzeraktionen wie das Ein- oder Ausschalten des Paket-Loggings.
System-Ereignisse	Der System-Log zeichnet automatisch fortlaufend Systemereignisse wie z. B. den Start eines Prozesses oder Aktionen, bei denen sich ein Benutzer nicht korrekt über Passwort authentisiert hat, auf. Anhand von Ereignisklassen ist die Aufzeichnung skalierbar.
	Leitungsdiagnose: Zusätzlich ist eine Leitungsdiagnose projektierbar. Die Leitungsdiagnose liefert Meldungen, sobald die Anzahl fehlerhafter Telegrammpakete einen einstellbaren Grenzwert überschritten hat.

Speicherverfahren für die Datenaufzeichnung beim lokalen Logging

Die Speicherung bei der Datenaufzeichnung erfolgt nach zwei wählbaren Verfahren:

- Umlaufspeicher

Bei Erreichen des Pufferendes wird die Aufzeichnung am Pufferanfang mit dem Überschreiben der ältesten Einträge fortgesetzt.

- Linearer Speicher

Die Aufzeichnung stoppt, wenn der Puffer voll ist.

Ein- bzw. Ausschalten des Logging

Im Erweiterten Modus können Sie in der Betriebsart "Offline" über die Log-Einstellungen in den Baugruppeneigenschaften das lokale Logging für die Ereignisklassen aktivieren und das Speicherverfahren festlegen. Diese Log-Einstellungen werden mit der Konfiguration in die Baugruppe geladen und werden mit dem Start der Security-Baugruppe wirksam.

Sie können das lokale Logging für Paketfilter-Ereignisse und System-Ereignisse in den Online-Funktionen bei Bedarf ebenfalls aktivieren oder deaktivieren. Die Einstellungen in der Projektkonfiguration werden dadurch nicht verändert.

Anzeige des Aufzeichnungszustands

Online-Einstellungen werden nicht in der Konfiguration gespeichert.

9.2.1 Lokales Logging - Einstellungen in der Konfiguration

In der Betriebsart "Offline" können Sie über die Log-Einstellungen die Ereignisklassen aktivieren und das Speicherverfahren festlegen. Diese Log-Einstellungen werden mit der Konfiguration auf die Baugruppe geladen und werden mit dem Start der Security-Baugruppe wirksam.

Sie können diese projektierten Log-Einstellungen in den Online-Funktionen bei Bedarf ändern. Die Einstellungen in der Projektkonfiguration werden dadurch nicht verändert.

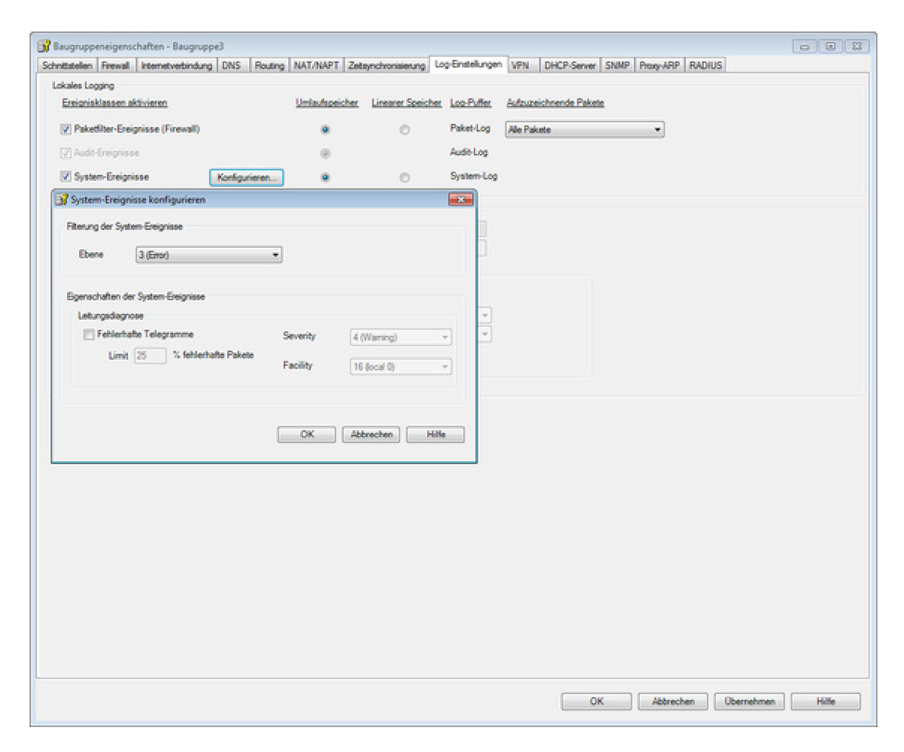
Log-Einstellungen im Standard Modus

Die Log-Einstellungen im Standard Modus entsprechen den Voreinstellungen im Erweiterten Modus. Im Standard Modus können Sie die Einstellungen jedoch nicht verändern.

Log-Einstellungen im Erweiterten Modus

1. Markieren Sie die zu bearbeitende Baugruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Log-Einstellungen".

Der folgende Dialog zeigt die Standard-Einstellungen für die Security-Baugruppe; zusätzlich ist der Dialog zur Konfiguration der Aufzeichnung von System-Ereignissen geöffnet:



Ereignisklassen konfigurieren

Tabelle 9- 2 Lokaler Log - Funktionsübersicht

Funktion / Register im Online-Dialog	Projektierung	Bemerkungen
Paketfilter-Ereignisse (Firewall)	Die Aktivierung erfolgt über Optionskästchen. Die Auswahl des Speicherverfahrens erfolgt über Optionsfelder. Aus der Klappliste "Aufgezeichnete Pakete" können Sie die Menge aufgezeichneter Datenpakete festlegen: • "Alle Pakete": Es werden die Datenpakete aufgezeichnet, auf die eine projektierte Firewall-Regel (Standard Modus oder Erweiterter Modus) zutrifft. Zusätzlich werden die Antwortpakete auf solche Pakete aufgezeichnet, welche die Firewall gemäß einer projektierten Allow-Regel passiert haben. • "Zustandserzeugende Pakete": Es werden ausschließlich die Datenpakete aufgezeichnet, auf die eine projektierte Firewall-Regel (Standard Modus oder Erweiterter Modus) zutrifft.	Paketfilter-Logdaten sind nicht remanent Die Daten werden in einem flüchtigen Speicher der Security-Baugruppe abgelegt und stehen deshalb nach einem Ausschalten der Spannungsversorgung nicht mehr zur Verfügung.
Audit-Ereignisse (immer aktiviert)	Logging ist immer aktiviert. Die Speicherung erfolgt immer im Umlaufpuffer.	Audit-Logdaten sind remanent Die Daten werden in einem remanenten Speicher der Security-Baugruppe abgelegt und stehen deshalb auch nach einem Ausschalten der Spannungsversorgung noch zur Verfügung. **Hinweis für CPs:** Die Audit-Logdaten sind bei CPs nicht remanent. Zur Sicherung der Daten sollte deshalb ein Syslog-Server verwendet werden.
System-Ereignisse	Die Aktivierung erfolgt über Optionskästchen. Die Auswahl des Speicherverfahrens erfolgt über Optionsfelder. Zur Konfiguration des Ereignisfilters und der Leitungsdiagnose öffnen Sie über die Schaltfläche "Konfigurieren..." einen weiteren Dialog.	System-Logdaten sind nicht remanent Die Daten werden in einem flüchtigen Speicher der Security-Baugruppe abgelegt und stehen deshalb nach einem Ausschalten der Spannungsversorgung nicht mehr zur Verfügung.

Funktion / Register im Online-Dialog	Projektierung	Bemerkungen
Filterung der System-Ereignisse	Stellen Sie in diesem Sub-Dialog für die System-Ereignisse eine Filterebene ein. Standardmäßig sind die folgenden Werte eingestellt: • SCALANCE S: Ebene 3 • CP: Ebene 3	Wählen Sie als Filterebene "Error" oder einen höheren Wert, um die Aufzeichnung von allgemeinen, nicht kritischen Ereignissen abzustellen. **Hinweis für CP** Wählen Sie für den CP nur Ebene 3 oder Ebene 6 aus. • Bei Auswahl von Ebene 3 werden die Fehlermeldungen der Ebenen 0 bis 3 ausgegeben. • Bei Auswahl von Ebene 6 werden die Fehlermeldungen der Ebenen 0 bis 6 ausgegeben.
Leitungsdiagnose CP	Die Leitungsdiagnose erzeugt ein spezielles System-Ereignis. Stellen Sie ein, ab welchem Prozentsatz fehlerhafter Telegramme ein System-Ereignis erzeugt werden soll. Weisen Sie dem System-Ereignis eine Facility und eine Severity zu.	Über die Severity gewichten Sie die System-Ereignisse der Leitungsdiagnose im Verhältnis zur Severity der übrigen System-Ereignisse. **Hinweis** Weisen Sie den System-Ereignissen der Leitungsdiagnose keine geringere Severity als der Filterung der System-Ereignisse zu. Ansonsten passieren diese Ereignisse den Filter nicht und werden nicht aufgezeichnet.

9.2.2 Netzwerk-Syslog - Einstellungen in der Konfiguration

Sie können die Security-Baugruppe als Client konfigurieren, der Logging-Informationen an einen Syslog-Server sendet. Der Syslog-Server kann sich im lokalen internen oder im externen Subnetz befinden. Die Implementierung entspricht RFC 3164.

Hinweis

Firewall - Syslog-Server im externen Netz nicht aktiv

Wenn der Syslog-Server auf dem adressierten Rechner nicht aktiv ist, sendet dieser Rechner in der Regel ICMP-Antworttelegramme "port not reachable" zurück. Wenn aufgrund der Firewall-Konfiguration diese Antworttelegramme als Systemereignisse aufgezeichnet und an den Syslog-Server gesendet werden, kann sich dieser Vorgang endlos fortsetzen (Ereignis-Lawine).

Abhilfen:

- Syslog-Server starten;
- Firewall-Regeln ändern;
- Rechner mit deaktiviertem Syslog-Server vom Netz nehmen.

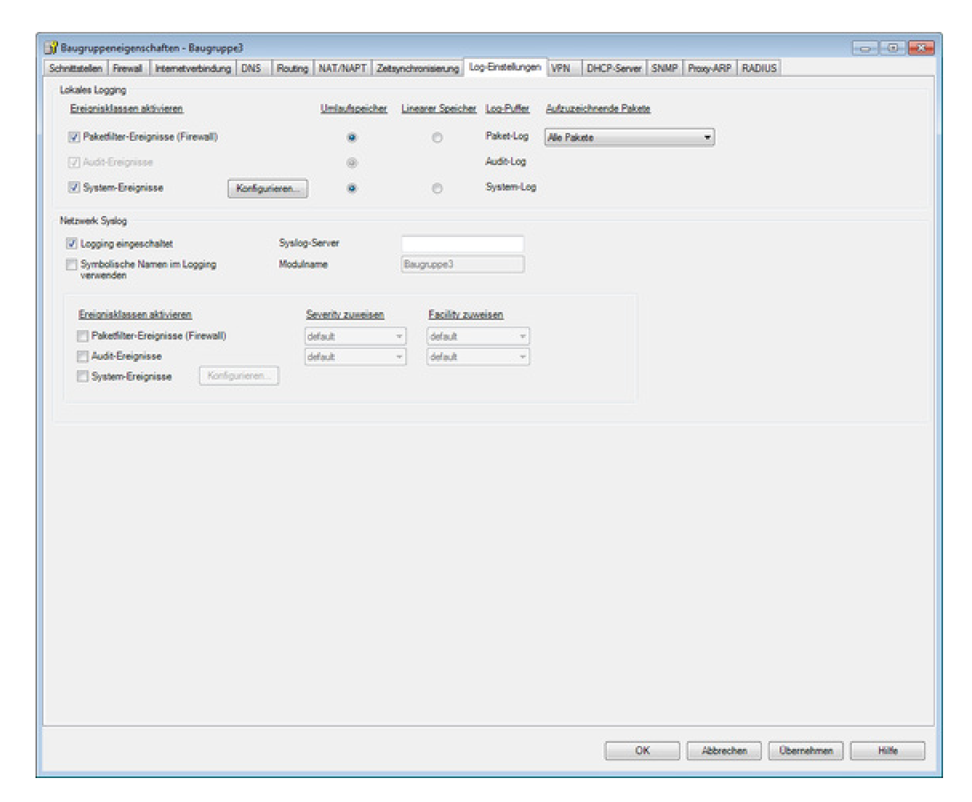
Log-Einstellungen vornehmen

1. Schalten Sie über den Menübefehl "Ansicht" > "Erweiterter Modus" die Betriebsart um.

> **Hinweis**
>
> **Keine Umschaltung zurück in den Standard Modus möglich**
>
> Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.
>
> Abhilfe SCT Standalone: Sie schließen das Projekt ohne zu speichern und öffnen Sie es erneut.

2. Markieren Sie die zu bearbeitende Security-Baugruppe.
3. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Log-Einstellungen".

Der folgende Dialog zeigt die Standard-Einstellungen für die Security-Baugruppe bei aktiviertem Logging für das Netzwerk Syslog:



Verbindung zum Syslog-Server herstellen

Für SCALANCE S: Die Security-Baugruppe verwendet den projektierten Baugruppennamen als Hostnamen gegenüber dem Syslog-Server.

Für CPs: Die Security-Baugruppe verwendet die eigene IP-Adresse als Hostnamen gegenüber dem Syslog-Server.

Geben Sie im Feld "Syslog-Server" die IP-Adresse / den FQDN des Syslog-Servers ein. Sie können die IP-Adresse alternativ als symbolischen Namen oder numerisch eingeben.

Der Syslog-Server muss von der Security-Baugruppe aus über die angegebene IP-Adresse erreichbar sein, ggf. über die Router-Projektierung im Register "Routing". Wenn der Syslog-Server nicht erreichbar ist, wird das Versenden der Syslog-Informationen abgeschaltet. Sie können diesen Betriebszustand anhand entsprechender Systemmeldungen erkennen. Um das Versenden der Syslog-Informationen erneut zu aktivieren, müssen Sie ggf. die Routing-Informationen aktualisieren und einen Neustart des Security-Moduls veranlassen.

Symbolische Namen im Logging verwenden



Aktivieren Sie das Optionskästchen "Symbolische Namen im Logging verwenden", werden die an den Syslog-Server übermittelten Adressangaben der Log-Telegramme durch symbolische Namen ersetzen. Die Security-Baugruppe prüft, ob entsprechende symbolische Namen projektiert sind und trägt diese in die Log-Telegramme ein.

Hinweis

Höhere Bearbeitungszeit bei symbolischen Namen

Ist das Optionskästchen "Symbolische Namen im Logging verwenden" aktiviert, wird die Bearbeitungszeit in der Security-Baugruppe erhöht.

Für die IP-Adressen der Security-Baugruppen werden automatisch die Baugruppennamen als symbolische Namen verwendet. Im Routing-Modus werden diese Namen mit einer Port-Bezeichnung wie folgt erweitert: "Baugruppenname-P1", "Baugruppenname-P2" usw.

Ereignisklassen konfigurieren

Tabelle 9- 3 Netzwerk Syslog - Funktionsübersicht

Funktion / Register im Online-Dialog	Projektierung	Bemerkungen
Paketfilter-Ereignisse (Firewall)	Die Aktivierung erfolgt über das Optionskästchen. Durch die Einstellung von Facility und Severity lassen sich Syslog-Meldungen entsprechend ihrer Herkunft und ihres Schweregrades klassifizieren. Die Zuordnung erfolgt über Klapplisten. Jedem Ereignis wird die Severity und Facility zugewiesen, die Sie hier einstellen.	Welchen Wert Sie hier wählen, hängt von der Auswertung im Syslog-Server ab. Damit können Sie eine Anpassung an die Erfordernisse im Syslog-Server vornehmen. Lassen Sie den Standardwert "default" eingestellt, wird durch die Security-Baugruppe festgelegt, mit welcher Kombination aus Facility und Severity das Ereignis angezeigt wird.
Audit-Ereignisse	Die Aktivierung erfolgt über das Optionskästchen. Die Zuordnung der Severity und Facility erfolgt über Klapplisten. Jedem Ereignis wird die Severity und Facility zugewiesen, die Sie hier einstellen.	Welchen Wert Sie hier für Severity und Facility wählen, hängt von der Auswertung im Syslog-Server ab. Damit können Sie eine Anpassung an die Erfordernisse im Syslog-Server vornehmen. Lassen Sie den Standardwert "default" eingestellt, wird durch die Security-Baugruppe festgelegt, mit welcher Kombination aus Facility und Severity das Ereignis angezeigt wird.
System-Ereignisse	Die Aktivierung erfolgt über das Optionskästchen.	Zur Konfiguration des Ereignisfilters und der Leitungsdiagnose öffnen Sie über die Schaltfläche "Konfigurieren..." einen weiteren Dialog.

Funktion / Register im Online-Dialog	Projektierung	Bemerkungen
Filterung der System-Ereignisse	Stellen Sie in diesem Sub-Dialog für die Systemereignisse eine Filterebene ein. Standardmäßig sind die folgenden Werte eingestellt: • SCALANCE S: Ebene 3 • CP: Ebene 3	Wählen Sie als Filterebene "Error" oder einen höheren Wert, um die Aufzeichnung von allgemeinen, nicht kritischen Ereignissen abzustellen. **Hinweis für CP** Wählen Sie für den CP nur Ebene 3 oder Ebene 6 aus. • Bei Auswahl von Ebene 3 werden die Fehlermeldungen der Ebenen 0 bis 3 ausgegeben. • Bei Auswahl von Ebene 6 werden die Fehlermeldungen der Ebenen 0 bis 6 ausgegeben.
Leitungsdiagnose CP	Die Leitungsdiagnose erzeugt ein spezielles System-Ereignis. Stellen Sie ein, ab welchem Prozentsatz fehlerhafter Telegramme ein System-Ereignis erzeugt werden soll. Weisen Sie dem System-Ereignis eine Facility und eine Severity zu.	Über die Severity gewichten Sie die System-Ereignisse der Leitungsdiagnose im Verhältnis zur Severity der übrigen System-Ereignisse. **Hinweis** Weisen Sie den System-Ereignissen der Leitungsdiagnose keine geringere Severity als der Filterung der System-Ereignisse zu. Ansonsten passieren diese Ereignisse den Filter nicht und werden vom Syslog-Server nicht aufgezeichnet.

9.2.3 Projektierung des Paket-Logging

Projektierung des Logging im Standard Modus

Informationen zum Logging von IP- und MAC-Regelsätzen finden Sie in folgenden Kapiteln:

- SCALANCE S im Standard Modus (Seite 128)
- CPs im Standard Modus (Seite 117)

Hinweis



Zusammenhang zwischen Log-Einstellungen im Standard Modus und Firewall-Regeln

Log-Einstellungen im Standard Modus wirken nicht für Firewall-Regeln, die durch eine Verbindungsprojektierung automatisch erzeugt wurden. So können beispielsweise getunnelte Telegramme einer projektierten Verbindung nicht geloggt werden. Im Erweiterten Modus kann das Logging auf die automatisch erzeugten Firewall-Regeln von Verbindungen ausgeweitet werden.

Projektierung des Logging im Erweiterten Modus

Die Aktivierung des Logging ist für beide Regeltypen (IP oder MAC) und alle Regeln identisch. Um Datenpakete bestimmter Paketfilter-Regeln aufzuzeichnen, setzen Sie im Register "Firewall" in der Spalte "Logging" einen Auswahlhaken.

Anhang A

A.1 DNS-Konformität

DNS-Konformität gemäß RFC1035 beinhaltet folgende Regeln:

- Beschränkung auf 255 Zeichen insgesamt (Buchstaben, Ziffern, Bindestrich oder Punkt);
- der Name muss mit einem Buchstaben beginnen;
- der Name darf nur mit einem Buchstaben oder einer Ziffer enden;
- ein Namensbestandteil innerhalb des Namens, d. h. eine Zeichenkette zwischen zwei Punkten, darf max. 63 Zeichen lang sein;
- keine Sonderzeichen wie Umlaute, Klammern, Unterstrich, Schrägstrich, Blank etc.

A.2 Wertebereiche IP-Adresse, Subnetzmaske und Adresse des Netzübergangs

Wertebereich für IP-Adresse

Die IP-Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 141.80.0.16

Wertebereich für Subnetzmaske

Die Subnetzmaske besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 255.255.0.0

Die 4 Dezimalzahlen der Subnetzmaske müssen in ihrer binären Darstellung von links eine Folge von lückenlosen Werten "1" und von rechts eine Folge von lückenlosen Werten "0" enthalten.

Die Werte "1" bestimmen die Netznummer innerhalb der IP-Adresse. Die Werte "0" die Host-Adresse innerhalb der IP-Adresse.

Beispiel:

richtige Werte:

255.255.0.0 Dezimal = 11111111.11111111.00000000.00000000 Binär

255.255.128.0 Dezimal = 11111111.11111111.10000000.00000000 Binär

255.254.0.0 Dezimal = 11111111.11111110.00000000.00000000 Binär

falscher Wert:

255.255.1.0 Dezimal = 11111111.11111111.00000001.00000000 Binär

Zusammenhang IP-Adresse und Subnetzmaske

Die erste Dezimalzahl der IP-Adresse (von links) bestimmt den Aufbau der Subnetzmaske hinsichtlich der Anzahl der Werte "1" (binär) wie folgt (für "x" steht die Host-Adresse):

Erste Dezimalzahl der IP-Adresse	Subnetzmaske
0 bis 127	255.x.x.x
128 bis 191	255.255.x.x
192 bis 223	255.255.255.x

Hinweis:

Für die erste Dezimalzahl der IP-Adresse können Sie auch einen Wert zwischen 224 und 255 eintragen. Dies ist jedoch nicht empfehlenswert, da dieser Adressbereich für andere Aufgaben reserviert ist und bei einigen Konfigurationstools (z.B. STEP 7) für diese Werte keine Prüfung erfolgt.

Wertebereich für Adresse des Netzübergangs

Die Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 141.80.0.1

Zusammenhang IP-Adresse und Adresse des Netzübergangs

Die IP-Adresse und die Adresse des Netzübergangs dürfen nur an den Stellen unterschiedlich sein, an denen in der Subnetzmaske "0" steht.

Beispiel:

Sie haben eingegeben: für Subnetzmaske 255.255.255.0; für IP-Adresse 141.30.0.5 und für die Adresse des Netzübergangs 141.30.128.254. Die IP-Adresse und die Adresse des Netzübergangs dürfen nur in der 4. Dezimalzahl einen unterschiedlichen Wert haben. Im Beispiel ist aber die 3. Stelle schon unterschiedlich.

Im Beispiel müssen Sie also alternativ ändern:

die Subnetzmaske auf: 255.255.0.0 oder

die IP-Adresse auf: 141.30.128.5 oder

die Adresse des Netzübergangs auf: 141.30.0.254

A.3 MAC-Adresse

Hinweis zum Aufbau der MAC-Adresse:

MAC-Adressen sind Hardware-Adresse zur Identifikation von Netzwerkteilnehmern. Eine MAC-Adresse besteht aus sechs Bytes, die, durch Bindestriche getrennt, hexadezimal notiert werden.

Die MAC-Adresse besteht aus einem festen und einem variablen Teil. Der feste Teil ("Basis-MAC-Adresse") kennzeichnet den Hersteller (Siemens, 3COM, ...). Der variable Teil der MAC-Adresse unterscheidet die verschiedenen Ethernet-Teilnehmer.

Literaturverzeichnis

B

B.1 Einleitung - ohne CD/DVD

Auffinden der SIMATIC NET-Dokumentation

- **Kataloge**

  Die Bestellnummern für die hier relevanten Siemens-Produkte finden Sie in den folgenden Katalogen:

  – SIMATIC NET Industrielle Kommunikation / Industrielle Identifikation, Katalog IK PI

  – SIMATIC Produkte für Totally Integrated Automation und Micro Automation, Katalog ST 70

  Die Kataloge sowie zusätzliche Informationen können Sie bei Ihrer Siemens-Vertretung anfordern.

  Die Industry Mall finden Sie unter folgender Adresse im Internet:

  Link zur Siemens Industry Mall (http://www.siemens.com/industrymall)

- **Dokumentation im Internet**

  Die SIMATIC NET-Handbücher finden Sie auf den Internet-Seiten des Siemens Automation Customer Support:

  Link zum Customer Support (http://support.automation.siemens.com/WW/view/de)

  Navigieren Sie zur gewünschten Produktgruppe und nehmen Sie folgende Einstellungen vor:

  Register "Beitragsliste", Beitragstyp "Handbücher / Betriebsanleitungen"

- **Dokumentation in der STEP 7-Installation**

  Handbücher, die in der Online-Dokumentation der STEP 7-Installation auf Ihrem PG/PC vorhanden sind, finden Sie über das Startmenü ("Start" > "Alle Programme" > "Siemens Automation" > "Dokumentation").

Siehe auch

Link zur Dokumentation:
(http://www.automation.siemens.com/simatic/portal/html_00/techdoku.htm)

B.2 S7-CPs / Zur Projektierung, Inbetriebnahme und Nutzung des CP

/1/

SIMATIC NET
S7-CPs für Industrial Ethernet
Projektieren und in Betrieb nehmen
Handbuch Teil A - Allgemeine Anwendungen
Projektierungshandbuch
Siemens AG
(SIMATIC NET Manual Collection)
Im Internet unter folgender Beitrags-ID:
30374198 (http://support.automation.siemens.com/WW/view/de/30374198)

/2/

SIMATIC NET

S7-CPs für Industrial Ethernet

Handbuch Teil B

Gerätehandbuch

Siemens AG

(SIMATIC NET Manual Collection)

Im Internet finden Sie die Gerätehandbücher für die einzelnen CPs jeweils unter folgender Beitrags-ID:

CP 343-1 Advanced (GX31): 28017299
(http://support.automation.siemens.com/WW/view/de/28017299)

CP 443-1 Advanced (GX30): 59187252
(http://support.automation.siemens.com/WW/view/de/59187252)

B.3 Zur Projektierung mit STEP 7 / NCM S7

/3/

SIMATIC NET
NCM S7 für Industrial Ethernet
Erste Schritte
Siemens AG
(Bestandteil der Online-Dokumentation in STEP 7)

/4/

SIMATIC NET
PC-Stationen In Betrieb nehmen - Anleitung und Schnelleinstieg
Projektierungshandbuch
Siemens AG
(SIMATIC NET Manual Collection)
Im Internet unter folgender Beitrags-ID:
13542666 (http://support.automation.siemens.com/WW/view/de/13542666)

/5/

SIMATIC
Hardware konfigurieren und Verbindungen projektieren mit STEP 7
Siemens AG
(Teil des Dokumentationspakets "STEP 7-Grundwissen")
(Bestandteil der Online-Dokumentation in STEP 7)

B.4 S7-CPs Zur Montage und Inbetriebnahme des CP

/6/

SIMATIC S7
Automatisierungssystem S7-300

- CPU 31xC und 31x Aufbauen: Betriebsanleitung
  Beitrags-ID: 13008499 (http://support.automation.siemens.com/WW/view/de/13008499)
- Baugruppendaten: Referenzhandbuch
  Beitrags-ID: 8859629 (http://support.automation.siemens.com/WW/view/de/8859629)

Siemens AG

sowie

SIMATIC S7
Automatisierungssystem S7-400, M7-400

- Aufbauen: Installationshandbuch
  Beitrags-ID: 1117849 (http://support.automation.siemens.com/WW/view/de/1117849)
- Baugruppendaten: Referenzhandbuch
  Beitrags-ID: 1117740 (http://support.automation.siemens.com/WW/view/de/1117740)

Siemens AG

B.5 Zu Aufbau und Betrieb eines Industrial Ethernet-Netzes

/7/

SIMATIC NET
Handbuch Twisted Pair- und Fiber Optic Netze
Siemens AG
(SIMATIC NET Manual Collection)

B.6 SIMATIC- und STEP 7-Grundlagen

/8/

SIMATIC
Kommunikation mit SIMATIC
Systemhandbuch
Siemens AG
Beitrags-ID:
25074283 (http://support.automation.siemens.com/WW/view/de/25074283)

/9/

Dokumentationspaket "STEP 7-Grundwissen"

- Erste Schritte und Übungen mit STEP 7 (ID: 18652511 (http://support.automation.siemens.com/WW/view/de/18652511))
- Programmieren mit STEP 7 (ID: 18652056 (http://support.automation.siemens.com/WW/view/de/18652056))
- Hardware konfigurieren und Verbindungen projektieren mit STEP 7 (ID: 18652631 (http://support.automation.siemens.com/WW/view/de/18652631))
- Von S5 nach S7, Umsteigerhandbuch (ID: 1118413 (http://support.automation.siemens.com/WW/view/de/1118413))

Siemens AG
Bestellnummer 6ES7 810-4CA08-8AW0

(Bestandteil der Online-Dokumentation in STEP 7)

B.7 Industrielle Kommunikation Band 2

/10/

SIMATIC NET
Industrial Ethernet Netzhandbuch
Siemens AG

(SIMATIC NET Manual Collection)

Im Internet unter folgender Beitrags-ID: 27069465
(http://support.automation.siemens.com/WW/view/de/27069465)

B.8 Zur Konfiguration von PC-Stationen / PGs

/11/

SIMATIC NET
PC-Stationen in Betrieb nehmen - Anleitung und Schnelleinstieg
Projektierungshandbuch
Siemens AG
Beitrags-ID: 13542666 (http://support.automation.siemens.com/WW/view/de/13542666)

B.9 Zur Konfiguration von PC-CPs

/12/

SIMATIC NET Industrial Ethernet CP 1628

Kompaktbetriebsanleitung
Siemens AG

(SIMATIC NET Manual Collection)

Im Internet unter folgender Beitrags-ID: 56714413
(http://support.automation.siemens.com/WW/view/de/56714413)

B.10 SIMATIC NET Industrial Ethernet Security

/13/

SIMATIC NET Industrial Ethernet Security
SCALANCE S ab V3.0

Inbetriebnahme- und Montagehandbuch
Siemens AG

(SIMATIC NET Manual Collection)

Im Internet unter folgender Beitrags-ID: 56576669
(http://support.automation.siemens.com/WW/view/de/56576669)

/14/

SIMATIC NET Industrial Remote Communication
SCALANCE M-800

Projektierungshandbuch
Siemens AG

(SIMATIC NET Manual Collection)

Im Internet unter folgender Beitrags-ID: 78389151

Siehe auch

78389151 (http://support.automation.siemens.com/WW/view/de/78389151)

/15/

SIMATIC NET
Telecontrol SCALANCE M875

Betriebsanleitung
Siemens AG

(SIMATIC NET Manual Collection)

Im Internet unter folgender Beitrags-ID: 58122394
(http://support.automation.siemens.com/WW/view/de/58122394)

Index

K

L

M

N

O

P

R

S

T

U